

UK ABWR

Document ID	:	GA91-9101-0101-24000
Document Number	:	UE-GD-0208
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 24 : Design Basis Analysis



DISCLAIMERS

Proprietary Information

This document contains proprietary information of Hitachi-GE Nuclear Energy, Ltd. (Hitachi-GE), its suppliers and subcontractors. This document and the information it contains shall not, in whole or in part, be used for any purpose other than for the Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR. This notice shall be included on any complete or partial reproduction of this document or the information it contains.

Copyright

No part of this document may be reproduced in any form, without the prior written permission of Hitachi-GE Nuclear Energy, Ltd.

Copyright (C) 2017 Hitachi-GE Nuclear Energy, Ltd. All Rights Reserved.

Table of Contents

Executive Summaryiv

24.1 Introduction24.1-1

 24.1.1 Background 24.1-1

 24.1.2 Document Structure..... 24.1-1

24.2 Purpose and Scope.....24.2-1

 24.2.1 Purpose..... 24.2-1

 24.2.2 Scope..... 24.2-2

24.3 Safety Case Relating to Faults.....24.3-1

 24.3.1 Overview of Safety Case 24.3-1

 24.3.2 Identification of Faults..... 24.3-1

 24.3.3 Acceptance Criteria 24.3-3

 24.3.4 High Level Safety Functions and the SSCs that provide them 24.3-8

 24.3.5 Transient and Dose Analysis..... 24.3-16

 24.3.6 Results of the Design Basis Assessment and Fault-based View 24.3-17

 24.3.7 Assumptions and Limits and Conditions for Operation 24.3-18

 24.3.8 Assessment that risks are ALARP 24.3-20

24.4 Fault Identification and Grouping and Fault Schedule24.4-1

 24.4.1 Introduction..... 24.4-1

 24.4.2 Fault Identification Based on Logic Tree Analysis 24.4-1

 24.4.3 Types of Fault..... 24.4-5

 24.4.4 Completeness of the List of Initiating Events 24.4-6

 24.4.5 List of Bounding Faults 24.4-7

 24.4.6 Fault Schedule for UK ABWR..... 24.4-21

24.5 Design Basis Analysis for UK ABWR.....24.5-1

 24.5.1 Introduction..... 24.5-1

 24.5.2 Basic Policy of Design Basis Analysis 24.5-1

 24.5.3 Analysis Codes 24.5-5

24.6 Analysis Results and Fault-based View – Non-Isolation Events.....24.6-1

 24.6.1 Increase in Reactor Pressure 24.6-6

 24.6.2 Decrease in Reactor Coolant Flow Rate..... 24.6-10

 24.6.3 Increase in Reactor Coolant Flow Rate 24.6-13

 24.6.4 Decrease in Reactor Coolant Temperature 24.6-16

 24.6.5 Reactivity and Power Distribution Anomalies..... 24.6-30

24.7 Analysis Results and Fault-based View – Isolation Events24.7-1

24.7.1 Increase in Reactor Pressure	24.7-4
24.7.2 Decrease in Reactor Coolant Inventory (RPV Water Level Decrease Events) ...	24.7-10
24.7.3 Loss of Off-site Power	24.7-15
24.8 Analysis Results and Fault-based View – Loss of Coolant Events.....	24.8-1
24.8.1 Inadvertent Opening of a SRV	24.8-5
24.8.2 Medium LOCA inside Primary Containment	24.8-10
24.8.3 Large LOCA inside Primary Containment	24.8-21
24.8.4 LOCA outside Primary Containment	24.8-41
24.9 Analysis Results and Fault-based View – Common Cause and Multiple Failures.....	24.9-1
24.9.1 Anticipated Transient without Scram (ATWS).....	24.9-2
24.9.2 Station Blackout (SBO)	24.9-20
24.9.3 Common Cause Failures of C&I systems, Electrical Distribution Systems and Essential Services and Support Systems	24.9-35
24.10 Analysis Results and Fault-based View – Reactor Faults Other Than at Full Power	24.10-1
24.10.1 Faults Occurring in Partial Power Operation	24.10-2
24.10.2 Reactor Faults in Shutdown Modes.....	24.10-12
24.11 Analysis Results and Fault-based View – Non-Reactor Faults	24.11-1
24.11.1 SFP and Fuel Route Faults	24.11-1
24.11.2 Radioactive Waste System Leak or Failure	24.11-21
24.12 Performance of Class 2 SSCs in Frequent Faults.....	24.12-1
24.12.1 Demonstrating Diverse Provision of Fundamental Safety Functions for Frequent Faults.....	24.12-3
24.13 Post-Accident Management for Safe Shutdown Following Design Basis Faults.....	24.13-1
24.13.1 Normal shutdown	24.13-1
24.13.2 Non-Isolation Events	24.13-1
24.13.3 Isolation Events	24.13-2
24.13.4 Loss of Cooling Events.....	24.13-3
24.13.5 ATWS Events.....	24.13-3
24.13.6 SBO Events	24.13-4
24.14 Assumptions, Limits and Conditions for Operation.....	24.14-1
24.15 Summary of ALARP Justification	24.15-1
24.16 Conclusions	24.16-1
24.17 References	24.17-1

Appendix A Table of SFC ClaimsA-1
Appendix B Table of SPC Claims..... B-1
Appendix C Document MapC-1

Executive Summary

This analysis chapter describes the safety case relating to Design Basis Faults for UK ABWR. It demonstrates that the safety systems provided in the design, as described in the PCSR systems chapters, successfully control all transients and accidents that make up the design basis, in all operating modes.

A generic definition of design basis faults is presented in Chapter 5: General Design Aspects. Chapter 24: Design Basis Analysis, summarises the process that was applied to develop a comprehensive list of specific design basis faults, and how this was used to produce the generic UK ABWR Fault Schedule that lists all of the bounding design basis faults that require assessment for GDA.

Design basis events are analysed in a number of groups. The reactor faults considered include transients where the reactor system is not isolated from the turbine/condensate/feedwater systems, and transients where the reactor system and turbine/condensate/feedwater systems are isolated from one another. Other groups considered are; loss of coolant accidents; events where a number of systems fail simultaneously or consequentially, including Anticipated Transients Without Scram (ATWS) and Station Black Out (SBO); and faults occurring during shutdown and refuelling.

The chapter scope also includes non-reactor faults, which are faults in other systems where there are radioactive materials, such as the fuel route and the radioactive waste systems.

A number of analysis Acceptance Criteria are presented that define what “successful control” of design basis faults means for a number of potential concerns. These are, radiation exposure to the public and workforce; protection of the nuclear fuel; the integrity of the reactor coolant circuit boundary; confinement of radioactive materials; and protection of nuclear fuel during handling and storage. The results of the analyses presented in this chapter show that the relevant Acceptance Criteria are met for all design basis faults listed in the GDA Fault Schedule.

The various computer codes used in the analyses are discussed, showing their relevance to specific types of design basis event. The methodology, of necessity, also makes a number of assumptions, which are specified in this chapter, including application of the single failure criterion. All of the assumptions made are fully consistent with the design information and safety claims for frontline and support systems that are made in the PCSR systems chapters. Some of the analysis assumptions are identified as Limits and Conditions for Operation where appropriate.

An explanation is provided of how the design basis fault assessments presented in this chapter contribute to the overall ALARP justification for the UK ABWR.

It is acknowledged that further work will be required post-GDA to develop the design and fully incorporate site specific aspects. The contents of this chapter forms the basis for the ongoing design basis fault studies that will be required as the site specific design develops. This work will be the responsibility of any future licensee.

24.1 Introduction

Chapter 24 demonstrates that UK ABWR is tolerant to Design Basis (DB) faults that arise in the reactor, support systems and power conversion system or during operations such as handling of spent fuel or radioactive waste. Faults may occur because of failures or unplanned transients anywhere in these systems and for each there is a well-defined set that constitute the Design Basis. This chapter identifies all such events and demonstrates that the dose-risk targets in Chapter 5 and in the Nuclear Safety and Environmental Design Principles (NSEDPs) [Ref-24] are met and that risks are As Low as Reasonably Practicable (ALARP).

24.1.1 Background

An important part of the safety case is the demonstration that the reactor and supporting systems are fault tolerant.

The process of demonstrating fault tolerance starts with the systematic identification of reactor faults and other abnormal situations that might arise with a frequency above the Design Basis cut-off. These reactor faults are grouped according to the demands they place on protection systems, and bounding cases identified for each group. Transient analysis of these bounding cases is performed to demonstrate that, with protection and mitigation systems in operation, consequences are below the corresponding Design Basis dose targets and risks are ALARP. In practice this is achieved by demonstrating that all relevant acceptance criteria, as defined in this chapter, are met. Design Basis assessment is performed for all operating phases and all operating modes of the reactor.

Design Basis assessment is also performed for all sources of radioactivity outside of the reactor including spent fuel and radioactive waste handling and storage and follows the same basic process as outlined above. For some of these sources, the provision of safety systems is much simpler than for the reactor and appropriate acceptance criteria are often just that Design Basis dose targets are met and risks are ALARP.

24.1.2 Document Structure

Section 24.2 gives the purpose and scope of the chapter.

Section 24.3 gives an overview of the safety case relating to faults, showing the process covering:

- Identification of faults
- Acceptance criteria

- High level safety functions and the SSCs that provide them
- Transient and dose analysis
- Results of the design basis assessment and fault-based view
- Assumptions and limits and conditions for operation
- Assessment that risks are ALARP

Section 24.4 describes the fault identification and bounding process, and also gives the acceptance criteria for each fault. The faults identified are for all sources of radiation (Reactor, Spent Fuel Pool (SFP) and Radioactive Waste Systems) and for all operating modes of the plant (Start-up, Power operation, Shutdown, refuelling outage,).

The list of bounding faults is incorporated into the Fault Schedule which also identifies the safety measures claimed in each case to protect against or mitigate the consequences of the fault. (A safety measure is defined in GDA Safety Case Development Manual [Ref-23] as ‘a safety system, or a combination of procedures, operator actions and safety systems that protects against a radiological consequence, or a specific feature of plant designed to prevent or mitigate a radiological consequence by passive means’). The Fault Schedule for the UK ABWR is described in Section 24.4.

Design Basis transient analysis is performed for each bounding fault taking the action of identified safety measures into account to show that appropriate acceptance criteria are met in each case. The general approach to this transient analysis is described in Section 24.5, which includes descriptions of the computer codes used. The transient analysis of specific DB faults is described in sections corresponding to the fault type, as below:

- Section 24.6 Analysis Description and Results – Non-isolation Events
- Section 24.7 Analysis Description and Results – Isolation Events
- Section 24.8 Analysis Description and Results – Loss of Coolant Events
- Section 24.9 Analysis Description and Results – Common Cause and Multiple Failures
- Section 24.10 Analysis Description and Results – Reactor Faults Other Than at Full Power
- Section 24.11 Analysis Description and Results – Non-Reactor Faults

Section 24.12 provides evidence that Class 2 systems can perform adequately in their role of supporting Class 1 Structures, Systems and Components (SSCs) for frequent faults.

Section 24.13 describes post-accident management actions bring the plant to cold shutdown conditions for all accident types.

Limits and Conditions for Operation arising from the DB fault studies are described in Section 24.14, and the input to the overall ALARP assessment is given in Section 24.15. Conclusions based on the DB analysis results are presented in Section 24.16, and References are in Section 24.17.

Appendix A gives links to Safety Functional Claims in other PCSR chapters, Appendix B describes Safety Property Claims important for DB assessment and Appendix C gives the document map relevant to this chapter.

The initiating events listed in the Fault Schedule also provide the input for the generic UK ABWR Level 1 PSA. Operation of the claimed safety systems provide some of the success criteria for the PSA. The description of the PSA can be found in Generic PCSR Chapter 25: Probabilistic Safety Assessment.

Chapter 24 also has links to the following chapters of the Generic PCSR:

- Chapter 4 Safety Management throughout Plant Lifecycle – Definitions of Assumptions and Limits and Conditions for Operation
- Chapter 5 General Design Aspects – Categorisation of Safety Functions and Classification of SSCs
- Chapter 6 External Hazards – Input to Fault Schedule
- Chapter 7 Internal Hazards – Input to Fault Schedule
- Chapter 8 Structural Integrity – Reactor Coolant Circuit Integrity
- Chapter 11 Reactor Core - Fuel Limits
- Chapter 12 Reactor Coolant Systems, Reactivity Control Systems, and Associated Systems – Faults in normally operating systems, some protection systems
- Chapter 13 Engineered Safety Features – ESFs, consisting of the Emergency Core Cooling system (ECCS) and Containment systems
- Chapter 14 Reactor Control and Instrumentation – Actuation of ESFs
- Chapter 15 Electrical Power Supplies – Power supplies to ESFs, Loss of Off-site Power (LOOP) faults and Station Blackout (SBO) faults
- Chapter 16 Auxiliary Systems - Faults in normally operating systems
- Chapter 17 Steam and Power Conversion Systems - Faults in normally operating systems
- Chapter 18 Radioactive Waste Management – Non-reactor faults
- Chapter 19 Fuel Storage and Handling – Non-reactor faults (Fuel Handling and Export)
- Chapter 20 Radiation Protection – Dose assessment
- Chapter 26 Beyond Design Basis and Severe Accident Analysis

- Chapter 27 Human Factors – Human error evaluation and Human Based Safety Claims (HBSCs)
- Chapter 32 Spent Fuel Interim Storage (SFIS) – Non-reactor faults

The chapter is supported by a number of Topic Reports:

- Topic Report on Fault Assessment [Ref-3]
- Topic Report on Fault Assessment for SFP and Fuel Route [Ref-4] (see also Chapter 19)
- Topic Report on Design Basis Analysis [Ref-5]
- Topic Report on Design Basis Analysis for SFP and Fuel Route [Ref-15] (see also Chapter 19)
- Topic Report on SBO analysis [Ref-16]

This Chapter does not cover environmental and security aspects of the UK ABWR design. For links to GEP, and CSA documentation, please refer to PCSR Chapter 1. For GEP, where specific references are required, for example in Radioactive Waste Management, Radiation Protection and Decommissioning, these are included in the specific sections within the PCSR.

24.2 Purpose and Scope

24.2.1 Purpose

The purpose of this chapter is to demonstrate that the UK ABWR is tolerant to faults within the Design Basis as defined in Chapter 5 and the NSEDPs [Ref-24]. In order to do this, faults (or initiating events) are identified in a systematic and auditable way, and listed in the Fault Schedule, which is also an input to the PSA described in Chapter 25. For each fault or fault group, an estimate assessment is made of the initiating event frequency and unmitigated consequences, that is, consequences with no safety systems operating. Any faults that are assessed as having frequency greater than 10^{-5} /y and unmitigated consequences above the Basic Safety Level (BSL), as defined in Section 5.5 of Chapter 5 and the NSEDPs [Ref-24], are designated as Design Basis Faults. These DB faults are grouped according to the demands they place on safety systems and bounding or worst case faults identified for each group. For a group of faults, the bounding fault is analysed rather than each fault individually.

Design Basis transient analysis is performed for each bounding fault taking the action of identified safety measures into account to show that appropriate acceptance criteria are met in each case. As part of this demonstration, High Level Safety Functions (HLSFs) and performance requirements are identified for the safety systems involved and HBSCs are also identified relating to any operator actions that may be required. Finally, the risks posed by each fault are shown to be ALARP.

A similar process is followed for Design Basis faults for all other operating modes and for all other sources of radiation such as spent fuel and radioactive waste.

In fact, the analysis goes well beyond showing that risk-dose targets are met. Acceptance criteria are defined that ensure that the main barriers to the release of activity (fuel cladding, reactor coolant pressure boundary and containment) remain functional during and after a Design Basis accident. Provided at least one of these barriers remains intact, there will be no release of radioactivity and the dose targets would be automatically met. In fact, for all Design Basis accidents affecting the reactor, the Design Basis assessment shows that at least one of the three barriers does remain intact.

The analysis assumes the correct functioning of the various protection systems that may be called upon in a Design Basis accident. This correct functioning defines the minimum number of systems required to be operational and the minimum performance of those systems that is required. These requirements define the major claims on the safety systems that are substantiated in other parts of the PCSR and also provide the basis of the definition of Limits and Conditions for Operation (LCOs), as do initial conditions and other parameters used in the transient analysis.

24.2.2 Scope

The scope of the Design Basis analysis presented in this chapter is all operating modes of the reactor as defined in Generic PCSR Chapter 5:

- Start-up,
- Power operation,
- Hot shutdown,
- Cold shutdown and
- Refuelling outage

and all sources of radiation:

- Reactor,
- Spent fuel storage in SFP and fuel handling operations in the Reactor Building, and
- Radioactive Waste

Analysis of spent fuel storage in the Spent Fuel Interim Storage (SFIS) facility is in PCSR Chapter 32.

Unplanned transients and other abnormal situations for the reactor are identified and assessed under the following headings:

- Abnormal changes in the reactivity or power distribution in the core,
- Abnormal reactivity insertion or rapid change in reactor power
- Abnormal change in heat generation or removal in the core
- Loss of reactor cooling or considerable change in core cooling
- Abnormal change in reactor coolant pressure or reactor coolant inventory

All faults identified under these headings, which have frequency and consequences inside the Design Basis as defined in Chapter 5, Section 5.5 are assessed in this chapter and its supporting Level 2 Topic Reports. Faults associated with the storage and handling of spent fuel or radioactive waste system are identified in a similar manner.

24.3 Safety Case Relating to Faults

24.3.1 Overview of Safety Case

The objective of the Design Basis Assessment is to demonstrate that the UK ABWR is tolerant to Design Basis faults, that is, the protection systems provided in the design ensure that public and worker doses in all fault conditions are within limits and ALARP.

The process to perform this demonstration has several parts:

- (1) Identify all the faults that need to be considered in the design basis and list them in the Fault Schedule
- (2) Identify Acceptance Criteria as a test to determine if the protection against a particular fault is adequate
- (3) Identify High Level Safety Functions (HLSFs) that need to be provided to meet the Acceptance Criteria. Identify the Structures, Systems and Components (SSCs) that provide the HLSFs
- (4) Perform Transient and Dose Analyses to show that the Acceptance Criteria are met if the HLSFs are provided by the identified SSCs
- (5) Identify any Limits and Conditions for Operation needed to ensure that assumptions in the analysis will be adhered to during plant operation
- (6) Demonstrate that the residual risks from faults are As Low As Reasonably Practicable

This analysis forms an important input to the overall ALARP assessment for UK ABWR.

24.3.2 Identification of Faults

In order to be confident in the fault tolerance of the design, it is necessary to ensure that the identification of faults is systematic, comprehensive and auditable.

The Design Basis is defined in Chapter 5, Section 5.5. The Design Basis (DB) is the set of faults with initiating fault frequency greater than 10^{-5} /y and whose unmitigated or unprotected consequences would be greater than the BSL. Frequent DB faults are those with initiating fault frequency greater than 10^{-3} /y.

The unmitigated or unprotected consequences are the consequences that would occur if none of the SSCs providing HLSFs were taken into account.

Once these SSCs are taken into account, any fault sequence, that is, initiating fault plus failure of the relevant SSCs, whose sequence frequency is greater than 10^{-7} /y, is also taken to be within the design basis and further protective or mitigative systems provided to bring the sequence frequency below 10^{-7} /y.

The fault identification process used in this assessment (Section 24.4) is based on the use of logic trees as described in Section 24.4.2. The list of faults identified has then been checked for completeness by comparison with guidance provided by IAEA and by comparison with the US-ABWR DCD produced for approval by US NRC. This comparison is described in Section 24.4.4. The total list of faults is given in the Fault Schedule [Ref-3] and bounding faults listed in Section 24.4.5.

The faults are divided into a number of groups:

Reactor Faults

- Non-isolation events
- Isolation events
- Loss of coolant events
- Common cause and multiple failures
- Reactor faults other than at full power

Non-reactor faults

- Faults in the handling and storage of spent fuel (Fuel Route faults)
- Faults in the handling and storage of radioactive waste including operator exposure during operations (e.g. unauthorised access to high dose areas)

Hazards

- Internal hazards
- External hazards

and a number of bounding faults identified for each group. Bounding faults are those faults that place the maximum demand on the relevant safety systems. The bounding faults are analysed in detail against the Acceptance Criteria to cover the entire list of faults and show that the Acceptance Criteria are met for all faults. The bounding faults for reactor and non-reactor faults are listed in Table 24.4-1.

Internal hazards are hazards to the reactor, fuel route, SFIS or radioactive waste systems arising on-site, such as fire and flooding. Internal hazards are assessed in Chapter 7 of the PCSR.

External hazards are hazards to the reactor, fuel route, SFIS or radioactive waste systems arising off-site and outside the control of the future licensee. They may be naturally occurring, such as earthquakes or extreme weather, or man-made, such as accidental aircraft crash. External hazards are identified in Chapter 6 and, since the main protection is from civil structures, are assessed in Chapter 10 of the PCSR.

The complete list of faults identified through this process forms the basis of the Fault Schedule. The faults are grouped under the corresponding Bounding Fault with details of the key plant impacts of the fault and its estimated unmitigated dose and whether the fault is considered to be a frequent or infrequent fault. For each fault, the SSCs that are claimed to provide the Fundamental Safety Functions Reactivity control, Fuel cooling and Long term heat removal are identified including the Class 1 SSCs claimed as being the first line means of provision, the Class 2 SSCs claimed as being second-line or diverse means of provision and any Class 3 SSCs providing defence in depth.

In the analysis presented in this chapter, for infrequent faults, only the Class 1 SSCs are claimed in the analysis, any Class 2 or Class 3 SSCs being part of the ALARP case as providing defence in depth. For frequent faults, Class 2 SSCs are also claimed as the diverse provision required by the NSEDPs.

24.3.3 Acceptance Criteria

The transient analysis for each bounding fault is judged against a set of Acceptance Criteria which ensure that dose targets are met either directly or through the protection of the barriers to the release of radioactivity (fuel cladding, reactor coolant circuit boundary and containment). It is a significant claim in the UK ABWR safety case that, for all DB faults, the provision of HLSFs by Class 1 SSCs (and by Class 2 SSCs in the case of frequent faults) ensures that at least one barrier to the release of radioactive materials remains intact where releases could lead to doses to the public or workforce greater than the BSL in the NSEDP dose targets. The Acceptance Criteria are derived from SFCs relating to the barriers to release of activity made in Chapters 11, 12, 13 and 19 of this PCSR.

In showing that the Acceptance Criteria are met, the transient analysis supports the above claim.

Acceptance criteria relating directly to meeting NSEDP dose targets for the public or workers are designated as 'AC-D x'.

The DB analysis presented in this chapter demonstrates that the principal barriers to radiological releases (fuel cladding, reactor coolant circuit pressure boundary and containment) are not

compromised in any DB fault. The corresponding Acceptance Criteria reflect the claimed withstand capability of the principal barriers in terms of parameters modelled in the transient analysis. Simply put, if the transient analysis shows that the relevant parameter is within the limits expressed in the SFC and incorporated in the corresponding Acceptance Criteria, and then the corresponding barrier failure mechanism will not occur, that is, the transient analysis forms the evidence that substantiates the claim that the barrier does not fail.

Acceptance Criteria relating to the protection of barriers to radioactive release are designated as follows:

Fuel limits (fuel cladding protection)	‘AC-F x’	(Chapter 11, Appendix A)
Reactor coolant circuit boundary	‘AC-R x’	(Chapter 12, Appendix A)
Containment	‘AC-C x’	(Chapter 13, Appendix A)
Criticality (fuel cladding protection)	‘AC-N x’	(Chapter 19, Appendix A)
Water levels in reactor or SFP (fuel cladding protection)	‘AC-W x’	(Chapter 19, Appendix A)

24.3.3.1 Acceptance Criteria Relating to Radiation Exposure of Workers or the Public

The NSEDPs [Ref-24] specify limits for DB faults (NSEDP SP.14.2.1) and these limits are carried into the DB assessment as dose criteria:

- (AC-D1) Dose to workers should be less than 20 mSv for initiating event frequencies exceeding 1×10^{-3} /y.
- (AC-D2) Dose to members of the public should be less than 1 mSv for initiating event frequencies exceeding 1×10^{-3} /y.
- (AC-D3) Dose to workers should be less than 200 mSv for initiating event frequencies between 1×10^{-3} and 1×10^{-4} /y.
- (AC-D4) Dose to members of the public should be less than 10 mSv for initiating event frequencies between 1×10^{-3} and 1×10^{-4} /y.
- (AC-D5) Dose to workers should be less than 500 mSv for initiating event frequencies between 1×10^{-4} /y and 1×10^{-5} /y.
- (AC-D6) Dose to members of the public should be less than 100 mSv for initiating event frequencies between 1×10^{-4} /y and 1×10^{-5} /y.

All faults should meet criteria AC-D1 to AC-D6, although application of the ALARP principle leads to much lower doses being achieved in practice. For the reactor and SFP, more stringent criteria related to barriers to release of activity (fuel cladding, reactor pressure boundary and containment) are used so that there is no release of activity and no worker or public dose in DB faults. In these cases, AC-D1 and AC-D2 are met automatically and so are not listed for these faults; the more stringent criteria being listed instead. The dose-risk targets for workers and the public are also discussed in Chapter 20.

24.3.3.2 Acceptance Criteria Relating to Nuclear Fuel

In DB faults in the reactor and SFP, the first line of defence against radioactive release is the fuel cladding. The absolute criterion for this is that the maximum fuel cladding temperature should be such that excessive embrittlement of fuel cladding is prevented. All DB faults should therefore meet the criteria AC-F5 derived from FA SFC 2-1.1 (See Chapter 11, Appendix A) and AC-F4 derived from FA SFC 2-1.2 (See Chapter 11, Appendix A):

- (AC-F5) The calculated maximum fuel cladding temperature shall not exceed 1,200°C.
- (AC-F4) The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

The ALARP principle requires that the greatest margin to fuel cladding failure that is reasonably practicable should be adopted. For UK ABWR, the application of this principle leads to the requirement that, for frequent faults, there should be a greater margin to fuel failure than achieved through the above criteria. In these cases, boiling transition is allowed to occur however, fuel limits are applied so that there is no fuel cladding perforation. It is a requirement that frequent faults meet the criteria AC-F3 derived from THD SFC 2-1.2 (See Chapter 11, Appendix A) and AC-F2 derived from FA SFC 4-10.3 (See Chapter 11, Appendix A):

(AC-F3) The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning /creep rupture (perforation) temperature, so as to preclude cladding failure.

(AC-F2) Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the Thermal Over-Power (TOP) or the Mechanical Over-Power (MOP) limits.

FA SFC 4-10.3 is defined in terms of cladding circumferential strain due to pellet-clad mechanical interaction but is interpreted here as relating to the corresponding thermal and mechanical over-power limits.

For many transients, it is reasonably practicable to provide significantly greater margin than this by maintaining nucleate boiling for the entire transient. Where reasonably practicable, faults should meet the criterion AC-F1 derived from THD SFC 2-1.1 (See Chapter 11, Appendix A):

(AC-F1) The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.

The above criteria relate to the fuel cladding. For reactivity insertion faults and faults which severely distort the neutron flux shape, there is the possibility that energy deposited in the fuel may lead to fuel failure even if the cladding is otherwise intact. All DB faults should therefore meet the criterion AC-F7 and AC-F6 derived from FA SFC 2-1.3 (See Chapter 11, Appendix A):

(AC-F7) Fuel enthalpy shall not exceed the limit value to prevent the generation of mechanical energy in the case of reactivity insertion faults.

As above, the ALARP principle leads to the requirement that frequent faults meet the more stringent criterion:

(AC-F6) Fuel enthalpy shall not exceed the design limit in the case of a reactivity insertion fault.

For infrequent faults, the operation of the Class 1 safety systems is required to achieve the nuclear fuel acceptance criteria AC-F4, AC-F5 and AC-F7. For frequent faults, the operation of the Class 1

safety systems is required to achieve the nuclear fuel acceptance criteria AC-F2, AC-F3 (or AC-F1 if appropriate) and AC-F6. The demonstration that these acceptance criteria are met is given in the relevant sections of 24.6 through 24.10 in this chapter.

In the event of assumed failure of Class 1 safety systems for frequent faults, the operation of the Class 2 safety systems is required to meet the same criteria as infrequent faults, namely, AC-F4, AC-F5 and AC-F7. The demonstration of the action of Class 2 systems for frequent faults is given in Section 24.12.

24.3.3.3 Acceptance Criteria Related to Reactor Coolant Circuit Boundary Integrity

The second line of defence against the release of radioactivity for all non-LOCA faults is the reactor primary circuit boundary. For LOCA events, it is assumed that this boundary is failed and so no acceptance criteria relating to the coolant circuit boundary apply. However, for transients, it is a requirement that the coolant circuit integrity be maintained through the use of the criterion AC-R1 and AC-R2 derived from NB SFC 4-2.1 (See Chapter 12, Appendix A and Section 12.3.3.3):

(AC-R2) Pressure on the reactor coolant pressure boundary shall be maintained below 120% of the maximum allowable working pressure.

As above, the ALARP principle leads to the requirement that frequent faults meet the more stringent criterion:

(AC-R1) Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.

24.3.3.4 Acceptance Criteria Related to Containment

The third line of defence against release of radioactivity is the containment boundary. All DB faults should meet the criterion AC-C1 derived from PCV SFC 4-7.2 (See Chapter 13, Appendix A and Section 13.3.2.1):

(AC-C1) Pressure and Temperature on the primary containment boundary shall be maintained below the maximum design pressure and temperature (See Chapter 13, Table 13.3-1).

It is noted that for transients with both success of Class 1 reactivity control and the reactor coolant circuit boundary being maintained, it is assumed that pressure on the primary containment will not increase significantly and so no acceptance criteria relating to the containment boundary apply. In the context of this Acceptance Criterion, “containment” includes all areas of the Primary Containment including Drywell and Wetwell.

24.3.3.5 Acceptance Criteria Relating to Reactor Shutdown Modes and Spent Fuel Storage and Handling

During the reactor shutdown modes and storage and handling of spent fuel, the fuel limits above are not appropriate for preventing the release of activity from the fuel. In these cases, fuel damage is prevented by preventing criticality and by keeping the fuel covered by water. Thus fuel storage and handling faults should meet the following criteria AC-N1 derived from SFS SFC 1-9.1 and SFS SFC 1-10.1 (See Chapter 19, Appendix A) and AC-W1 and AC-W2 derived from SFS SFC 2-4.1 and SFS SFC 4-7.1 (See Chapter 19, Appendix A). The Fuel export canister should meet AC_C2 related to SFE-SFC_5-22.1:

(AC-N1) k_{eff} shall be smaller than 0.95 to maintain sub-criticality in the SFP.

(AC-W1) Reactor Pressure Vessel (RPV) water level shall be maintained above the Top of Active Fuel (TAF) of the reactor core during shutdown to prevent the fuel being uncovered and heating up.

(AC-W2) SFP water level shall be maintained above the TAF of the spent fuel pool to prevent spent fuel being uncovered and heating up.

(AC-C2) Canister deceleration following a DB drop shall remain below allowable limit.

The exact canister to be used for movement of spent fuel from the SFP has not been decided during GDA. Therefore, numerical values for the allowable limits for the canister cannot be determined at this stage.

24.3.4 High Level Safety Functions and the SSCs that provide them

The safe and controllable shutdown state for reactor design basis faults is achieved by the three Fundamental Safety Functions (FSFs) - reactivity control, reactor core cooling, and long-term heat removal - as described in Chapter 5. These FSFs are associated with HLSFs provided by a number of SSCs as described in Chapters 12, 13, 14, 15 and 16 of this PCSR for the reactor and Chapters 18 and 19 for radioactive waste and Fuel Route, respectively.

Even though the FSFs may be capable of being provided by a number of SSCs of different classes, only the Class 1 SSCs, that is the SSCs designed to provide protection against DB faults, are claimed in the analysis – even though lower class SSCs might be available, they are ignored in the analysis. For frequent faults, there is a requirement to provide diverse means of protection for each FSF to ensure that the sequence frequency target of 10^{-7} /y is met. These SSCs must be Class 2 as a minimum and a separate analysis (Section 24.12) demonstrates that corresponding Acceptance Criteria can be met when only these SCCs are claimed. The transient analysis demonstrates that the Acceptance Criteria are met for all DB faults protected by the corresponding SSCs providing the

identified HLSFs. If the Acceptance Criteria are met, then the claim that at least one barrier remains to prevent radiological release is met.

The following Table summarises key SSCs identified in the fault schedule for reactor DB faults and the HLSFs they provide as defined in Chapter 5, Table 5.6-1.

Table 24.3-1: Provision of Safety Functions

Reactivity Control - Reactor		HLSFs provided
Class 1	<ul style="list-style-type: none">Control Rod and Control Rod Drive System (CRD) (see Section 11.5.2, 12.4.3.1)	1-3
Class 2	<ul style="list-style-type: none">Standby Liquid Control System (SLC) (see Section 11.5.3 and 12.4.3.2)Alternative Rod Insertion (ARI) (see Section 11.5.2, 12.4.3.1 and 14.6.3)Recirculation Pump Trip (RPT) (see Section 14.6.3)Feed water Stop (see Section 14.6.3)	1-5

Table 24.3-1: Provision of Safety Functions (Continued)

Fuel Cooling - Reactor		HLSFs provided
Class 1	<ul style="list-style-type: none"> • Reactor Core Isolation Cooling System (RCIC) (see Section 13.4.1) • High Pressure Core Flooder System (HPCF) (see Section 13.4.1) • Safety Relief Valve (SRV) -Safety valve function- (see Section 12.3.3) <p>Protection against infrequent LOCA fault group:</p> <p>The Emergency Core Cooling System (ECCS) comprising the following systems</p> <ul style="list-style-type: none"> • Reactor Core Isolation Cooling System (RCIC) (see Section 13.4.1) • High Pressure Core Flooder System (HPCF) (see Section 13.4.1) • Low Pressure Core Flooder System (LPFL) (see Section 13.4.1) • Automatic Depressurisation System (ADS) (see Section 12.3.3 and 13.4.1) • Transient Automatic Depressurisation System (Transient ADS) (see Section 12.3.3 and 13.4.1) • Safety System and Logic Control (SSLC) (see Section 14.6.2.1) 	2-1
Class 2	<ul style="list-style-type: none"> • Reactor Depressurisation Control Facility (RDCF) (Alternative SRV) (see Section 16.7.3.3) • Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1) • Hard-Wired Backup System (HWBS) (see Section 14.6.3) 	2-2
Class 3	<ul style="list-style-type: none"> • Reactor Depressurisation Control Facility (Switching Valve for SRV) (RDCF) (see Section 16.7.3.3) 	2-2

Table 24.3-1: Provision of Safety Functions (Continued)

Long-term Heat Removal - Reactor		HLSFs provided
Class 1	<ul style="list-style-type: none"> • Safety Relief Valve (SRV) –Manual depressurisation– (see Section 12.3.5.2) • Residual Heat Removal System (RHR) (see Section 12.3.5.4) • Safety System and Logic Control (SSLC) (see Section 14.6.2.1) 	3-1
Class 2	<ul style="list-style-type: none"> • Atmospheric Control System (AC) (see Section 13.3.3.4) • Filtered Containment Venting System (see Section 13.3.3.4) • Hard-Wired Backup System (HWBS) (see Section 14.6.3) 	3-2
Confinement /Containment of Radioactive Materials - Reactor		HLSFs provided
Class 1	• Safety Relief Valve (SRV) (See Section 12.3.5.2)	4-2
	<ul style="list-style-type: none"> • Primary Containment (see Section 13.3) • Main Steam Isolation Valve (MSIV) and Flow restrictors (see Section 12.3.5.2 and 14.6.2.1) • Primary Containment Isolation System (PCIS) (see Section 12.3, 12.4 and 13.3.3.2) 	4-7
Class 2	<ul style="list-style-type: none"> • Secondary Containment (see Section 13.3.4.1) • Reactor Area (R/A) Heating Ventilating and Air Conditioning System (HVAC) Isolation Damper (see Section 16.5) • Standby Gas Treatment System (SGTS) (see Section 13.3.4.2) 	4-7
Others - Reactor		HLSFs provided
Class 1	• Safety System and Logic Control (SSLC) (see Section 14.6.2.1)	5-1
	<ul style="list-style-type: none"> • Class 1 Electrical Power System (Class 1 EPS) including Emergency Diesel Generator (EDG) (see Section 15.3) • Reactor Building Cooling Water System (RCW) (see Section 16.3.2) • Reactor Building Service Water System (RSW) (see Section 16.3.2) • Ultimate Heat Sink (UHS) (see Section 16.3.1) 	5-2
	<ul style="list-style-type: none"> • Class 1 Heating Ventilating and Air Conditioning System (Class 1 HVAC) (see Section 16.5) • HVAC Emergency Cooling Water System (HECW) (see Section 16.3.5.1) 	5-18

Table 24.3-1: Provision of Safety Functions (Continued)

Others - Reactor		HLSFs provided
Class 2	<ul style="list-style-type: none"> • Hard-Wired Backup System (HWBS) (see Section 14.6.3) • Safety Auxiliary Control System (SACS) (see Section 14.6.4) 	5-1
	<ul style="list-style-type: none"> • B/B Class 2 Electrical Power System (B/B Class 2 EPS) including Backup Building Generator (BBG) (see Section 15.3) • Emergency Equipment Cooling Water System (EECW) (see Section 16.3.6) 	5-3
	<ul style="list-style-type: none"> • Flammability Control System (FCS) - Passive Autocatalytic Recombiners (PARs) (see Section 13.3.3.3) 	5-15
	<ul style="list-style-type: none"> • Class 2 (A2) Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5) • HVAC Backup Building Cooling Water System (HBCW) (see Section 16.3.5.3) 	5-18
Class 3	<ul style="list-style-type: none"> • Diverse Additional Generator (DAG) (see Section 15.5.5) 	5-3

Table 24.3-1: Provision of Safety Functions (Continued)

Reactivity Control - Shutdown Modes		HLSFs provided
Class 1	<ul style="list-style-type: none"> Control Rod and Control Rod Drive System (CRD) (see Section 11.5.2, 12.4.3.1) 	1-3, 1-4
Fuel Cooling and Long Term Heat Removal - Shutdown Modes		HLSFs provided
Class 1	<ul style="list-style-type: none"> High Pressure Core Flooder System (HPCF) (see Section 13.4.1) Low Pressure Core Flooder System (LPFL) (see Section 13.4.1) Safety System and Logic Control (SSLC) (see Section 14.6.2.1) 	2-1
Class 2	<ul style="list-style-type: none"> Reactor Depressurisation Control Facility (RDCF) (Alternative SRV) (see Section 16.7.3.3) Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1) Hard-Wired Backup System (HWBS) (see Section 14.6.3) 	2-2
Class 3	<ul style="list-style-type: none"> Reactor Depressurisation Control Facility (Switching Valve for SRV) (RDCF) (see Section 16.7.3.3) Flooder System of Reactor Building (FLSR) (see Section 16.7.3.2) Fire Protection System (see Section 16.6.3) 	2-2
Class 1	<ul style="list-style-type: none"> Safety Relief Valve (SRV) –Manual depressurisation– (see Section 12.3.5.2) Residual Heat Removal System (RHR) (see Section 12.3.5.4) Safety System and Logic Control (SSLC) (see Section 14.6.2.1) 	3-1
Class 2	<ul style="list-style-type: none"> Atmospheric Control System (AC) (see Section 13.3.3.4) Filtered Containment Venting System (see Section 13.3.3.4) Hard-Wired Backup System (HWBS) (see Section 14.6.3) 	3-2
Confinement /Containment of Radioactive Materials – Shutdown modes		HLSFs provided
Class 1	<ul style="list-style-type: none"> Primary Containment Isolation System (PCIS) (see Section 12.3, 12.4 and 13.3.3.2) 	4-7

Table 24.3-1: Provision of Safety Functions (Continued)

Others – Shutdown modes		HLSFs provided
Class 1	<ul style="list-style-type: none"> • Safety System and Logic Control (SSLC) (see Section 14.6.2.1) 	5-1
	<ul style="list-style-type: none"> • Class 1 Electrical Power System (Class 1 EPS) including Emergency Diesel Generator (EDG) (see Section 15.3) • Reactor Building Cooling Water System (RCW) (see Section 16.3.2) • Reactor Building Service Water System (RSW) (see Section 16.3.2) • Ultimate Heat Sink (UHS) (see Section 16.3.1) 	5-2
	<ul style="list-style-type: none"> • Remote Shutdown System (RSS) (see Section 14.6.2.2) 	5-5
	<ul style="list-style-type: none"> • Fuel Handling Machine (PCSR Section 19.6) 	5-6
	<ul style="list-style-type: none"> • Class 1 Heating Ventilating and Air Conditioning System (Class 1 HVAC) (see Section 16.5) • HVAC Emergency Cooling Water System (HECW) (see Section 16.3.5.1) 	5-18
	<ul style="list-style-type: none"> • Hard-Wired Backup System (HWBS) (see Section 14.6.3) 	5-1
Class 2	<ul style="list-style-type: none"> • B/B Class 2 Electrical Power System (B/B Class 2 EPS) including Backup Building Generator (BBG) (see Section 15.3) • Emergency Equipment Cooling Water System (EECW) (see Section 16.3.6) 	5-3
	<ul style="list-style-type: none"> • Class 2 (A2) Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5) • HVAC Backup Building Cooling Water System (HBCW) (see Section 16.3.5.3) 	5-18
	<ul style="list-style-type: none"> • Class 2 (A2) Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5) • HVAC Backup Building Cooling Water System (HBCW) (see Section 16.3.5.3) 	5-18

Table 24.3-1: Provision of Safety Functions (Continued)

Reactivity Control - SFP		HLSFs provided
Class 1	<ul style="list-style-type: none"> Spent Fuel Storage Pool (SFP) (see Section 19.8) 	1-19
Fuel Cooling - SFP		HLSFs provided
Class 1	<ul style="list-style-type: none"> Spent Fuel Storage Facility (SFS) (see Sections 19.8) Fuel Pool Cooling System (FPC) (see Section 19.9.2.1) Residual Heat Removal System (RHR) (see Section 12.3.5.4) Safety System and Logic Control (SSLC) (see Section 14.6.2.1) 	2-4
Class 2	<ul style="list-style-type: none"> Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1) Hard-Wired Backup System (HWBS) (see Section 14.6.3) 	2-5
Confinement /Containment of Radioactive Materials - SFP		HLSFs provided
Class 1	<ul style="list-style-type: none"> The check valves and syphon break system (FPC) (see Section PCSR Section 19.9) Spent Fuel Storage Pool (SFP) (see Section 19.8) 	4-7
Class 2	<ul style="list-style-type: none"> Secondary Containment (see Section 13.3.4.1) Reactor Area (R/A) Heating Ventilating and Air Conditioning System (HVAC) Isolation Damper (see Section 16.5) Standby Gas Treatment System (SGTS) (see Section 13.3.4.2) 	4-7
Others - SFP		HLSFs provided
Class 2	<ul style="list-style-type: none"> Safety Auxiliary Control System (SACS) (see Section 14.6.4) 	5-1
Fuel Route Faults		HLSFs provided
Class 1	<ul style="list-style-type: none"> Fuel Handling Machine (FHM) (see Section 19.6) Reactor Building Overhead Crane (RBC) (see Section 19.7) 	5-6

Table 24.3-1: Provision of Safety Functions (Continued)

Spent Fuel Export and Radioactive Waste Handling and Storage		HLSFs provided
Class 1	• Canister basket (see Section 19.10)	1-10
	• Canister (see Section 19.10)	2-6, 4-14, 4-16, 5-16
	• Canister Cooling System (CCS) (see Section 19.10) • Over Temperature Protection System (OTPS) for Canister Drying (see Section 19.10)	2-6
	• Transfer Cask	4-16, 5-16
	• Reactor Building Overhead Crane (RBC) (see Section 19.7) • Fuel Handling Machine (FHM) (see Section 19.6) • Lifting Attachment (see Section 19.7)	5-6
	• Impact Limiters (see Section 19.10)	5-22
	Class 2	• Backup Canister Cooling System (BCCS) (see Section 19.10)
	• Cask stand (see Section 19.10)	5-16
Radioactive Waste Handling and Storage		HLSFs provided
Class 2	• Off Gas System isolation valve (OG isolation valve)	4-7

Infrequent DB faults are protected by the Class 1 SSCs in the above table. Frequent faults are additionally protected by the diverse Class 2 SSCs in the table to ensure that the sequence frequency target of 10^{-7} /y is also met. The Acceptance Criteria to ensure the adequacy of this diverse provision are less onerous than for the Class 1 SSCs.

In a number of faults, particularly during shutdown modes, there are instances where the above SSCs are initiated manually. These are noted in the appropriate places in this chapter and links are provided to the corresponding Human Based Safety Claim in Chapter 27.

24.3.5 Transient and Dose Analysis

Transient analysis is performed to model the plant behaviour following a DB initiating event as identified in the Fault Schedule. The design performance of the claimed SSCs is modelled and the

fault followed for sufficient time to demonstrate that the plant can be brought to a safe condition with the corresponding Acceptance Criteria being met.

The transient analysis is carried out using appropriate computer codes that model all of the important physical phenomena such as flow of water and steam in reactor, turbine (if appropriate) and containment, nuclear reactions, and heat transfer. (See Section 24.5.3)

The transient analysis uses standard computer codes designed to be used in Design Basis calculations. The codes have conservative models and use conservative data and assumptions to ensure that the results are bounding. The codes used in the DB transient analysis of UK ABWR are described in Section 24.5.3 and the policies on conservatism in the analysis is described in Section 24.5.2.

Most DB faults do not involve any release of radioactive materials. If the transient analysis indicates that radioactive material is released, for example because containment is bypassed, dose analysis is also performed.

Dose analysis starts with a conservative determination of the release using data on radioactive inventories discussed in Chapter 20 and 23. Any decontamination effects (e.g. deposition) are modelled using a suitable decontamination factor (DF). Dispersion and deposition inside buildings and in the environment are modelled using standard DB models and doses are then calculated for representative age groups (infant, child, adult) for the following pathways:

- Direct dose from cloudshine
- Inhalation dose
- Direct dose from groundshine
- Ingestion dose from contaminated foodstuffs

ICRP data is used for the dose coefficients corresponding to these pathways. A similar calculation is performed for operator doses, taking account of the effects of being inside a closed space, if appropriate, and also the effects of direct doses from equipment.

24.3.6 Results of the Design Basis Assessment and Fault-based View

The results of the DB analysis, showing that Acceptance Criteria are met and that, therefore, doses to workers and public are within NSEDP targets are given in the following sections:

- Non-isolation events – Section 24.6

- Isolation events – Section 24.7
- Loss of coolant events – Section 24.8
- Common cause and multiple failures – Section 24.9
- Reactor Faults other than at full power – Section 24.10
- Non-reactor faults – Section 24.11

The results in these sections are for the cases where HLSFs are provided by Class 1 SSCs. The demonstration that frequent fault Acceptance Criteria can be met by Class 2 SSCs is given in Section 24.12. Most transient analyses are terminated once the plant reaches a stable hot shutdown condition. The demonstration that the plant can be brought to a cold shutdown condition following these transients is given in Section 24.13.

24.3.7 Assumptions and Limits and Conditions for Operation

The analyses in this chapter make a number of assumptions and define a number of Limits and Conditions for Operation (LCOs) (Section 24.14). These assumptions and LCOs define a boundary within which the safety case relating to faults is valid. For GDA, it is assumed that the future licensee will operate the plant within this operating envelope (see Chapter 4, Section 4.12). In operation, if these LCOs are breached, then action must be taken within certain prescribed timescales to bring the operating envelope back within the bounds of the safety case. Otherwise, the reactor is operating without a valid Safety Case.

These LCOs have been identified following the standard procedure for GDA that is specified in [Ref-26], and are collated in the Generic Technical Specifications [Ref-27].

These assumptions and LCOs fall into three categories:

- (1) LCOs that define the initial conditions for faults
- (2) LCOs that guarantee the delivery of Safety Functions
- (3) LCOs that maintain accident doses within limits

(1) Assumptions and LCOs defining the initial conditions for the fault analysis

The transient analysis described in this chapter assumes certain starting conditions corresponding to worst case or conservative normal operating conditions. If the reactor is operated outwith these initial conditions, the conclusions of the transient analysis may not be valid. In the worst case, Acceptance Criteria may not be met in practice and release of activity may occur. If any parameter goes outside the prescribed range then corrective action needs to be taken within a prescribed

timescale to meet Design Basis requirements. These prescribed timescales are specified as ‘Completion times’ in [Ref-27].

Each fault or fault group in Sections 24.6 to 24.12 has a table “Analysis Conditions”, which lists the initial plant conditions such as pressures and flow rates assumed in the analysis. Some of these initial plant conditions are so important to the analysis that they are identified as LCOs. Less important assumptions are listed in the section “Analysis Assumptions” in each “Analysis of Event” section.

(2) Assumptions and LCOs that guarantee the delivery of HLSFs

These assumptions and LCOs mainly relate to the availability and performance of SSCs providing HLSFs. Ultimately, the assumptions and LCOs may form part of the Tech Specs for the reactor operation.

In all the DB transient calculation, it is assumed that at least one division of the claimed SSCs is available. As DB analysis is subject to the single failure criterion (that is, it is conservatively assumed that one whole division may be rendered unavailable by a single failure), every fault must have LCOs to ensure that one division remains available (for example by making sure that two divisions are not simultaneously being maintained or tested) and that safety property claims relating to defence in depth (SYS SPC 1), reliability (SYS SPC 3) and fault tolerance (SYS SPC 4) are satisfied.

Where a SSC is identified in a LCO, the LCO also applies to support systems in the same division.

In operation, if such an LCO is not complied with, corrective action needs to be taken within a prescribed timescale to meet Design Basis requirements. These prescribed timescales are specified as ‘Completion times’ in [Ref-27].

(3) Assumptions and LCOs that maintain accident doses within limits

For most DB faults, meeting the Acceptance Criteria ensure that barriers remain intact. These Acceptance Criteria therefore constitute assumptions and LCOs that maintain doses within limits. However, there are a small number of faults where other criteria also need to be met. For example, the dose may only be limited if a specific radioactive inventory as defined in the source term analysis in Chapter 20 is kept within the corresponding limit. For these faults, there is a LCO identified (or implied) that requires sampling and monitoring of reactor coolant, SFP or radioactive waste systems to ensure that the limit is not exceeded in operation. This sampling and monitoring is related to SFC RC SC 13.1 that the “chemistry sampling and monitoring system provides the analytical information of each SSCs associated with an Operating Rule” – see Chapter 23, Section 23.10.2.

In the particular case of LOCA events where containment is bypassed (LOCAs outside containment), the dose consequences are controlled by the control of activity in the fluid being discharged. The dominant sequence is main steam line break (MSLB) outside containment and the design basis Primary Source Term in Chapter 20 is chosen to reduce the doses from MSLB so far as is reasonably practicable. The LCO above on monitoring ensures that the reactor is operated within this limit.

In operation, if such as LCO is not complied with, corrective action needs to be taken within a prescribed timescale to meet Design Basis requirements. These prescribed timescales are specified as 'Completion times' in [Ref-27].

The LCOs identified in this chapter are cumulative and many apply to several, if not all, faults. Once they are identified in the chapter against a particular fault, they are not repeated in subsequent faults.

Ultimately, these assumptions and LCOs will need to be adopted by the future licensee to ensure that the reactor is operated within the bounds of the safety case, noting that the licensee has the option of revising the safety case to justify a different operating envelope.

24.3.8 Assessment that risks are ALARP

The analysis of DB faults shows that the Acceptance Criteria related to dose targets given in the NSEDPs are met for all DB faults. However, that demonstration is not adequate to provide a safety case with respect to faults. It is also necessary to demonstrate that the doses are As Low As Reasonably Practicable, that is, that doses cannot be further reduced by any reasonably practicable provision (Section 24.15).

There are a number of conservatisms that apply to the DB analysis that contribute to this demonstration:

- There are often large margins between calculated parameters and the corresponding Acceptance Criteria
- The DB analysis is very conservative meaning that calculated doses are significantly greater than would be realised in practice or that margins between calculated parameters and corresponding Acceptance Criteria are lower than would be realised in practice
- There are a number of SSCs of lower class that are not claimed in the analysis but would be available in practice and would make the consequences less likely, would make any doses less or would lead to greater margins to Acceptance Criteria being met

Even with these conservatisms, Acceptance Criteria are met indicating that it would be difficult to find additional protection measures to further reduce doses.

24. Design Basis Analysis

24.3 Safety Case Relating to Faults

Ver. 0

24.3-20

In addition, each SSC has been subject to an ALARP demonstration, reported in the relevant chapter of the PCSR. This demonstration concludes that there are no reasonably practicable means to make the SSC provide its corresponding HLSF with better performance or greater reliability.

Based on these considerations, the conclusion of this chapter in Section 24.15 is that there are no further reasonably practicable means that could be introduced to further reduce doses to workers or the public and, therefore, that these doses are ALARP. This conclusion feeds into the overall ALARP assessment for UK ABWR given in Chapter 28.

24.4 Fault Identification and Grouping and Fault Schedule

24.4.1 Introduction

The safety systems of UK ABWR plant are designed such that the extent of environmental release of any radioactive material from the plant during all operating modes is ALARP. A systematic approach to plant safety has been applied to the UK ABWR to ensure the list of Initiating Events and Bounding Faults is comprehensive in order to demonstrate the adequacy of the safety design and the suitability and sufficiency of the safety measures. Therefore, evaluation of initiating events and bounding faults in all operating modes, including those not directly related to the reactor, are performed by undertaking logic tree analysis, supplemented by the following:

- Comparison with International Atomic Energy Agency (IAEA) and US Design Control Document (US-DCD) approaches
- Failure Modes and Effects Analysis (FMEA), etc. for the UK ABWR

Nuclear power plants are designed to cope with, or are shown to withstand, a wide range of faults without unacceptable consequences by virtue of the facility's inherent characteristics or provision of safety functions. If the abnormal conditions are inadequately addressed or neglected, these faults may lead to the more severe damage to nuclear fuel or to the reactor coolant pressure boundary, and potentially lead to unacceptable release of radioactive materials from the nuclear facility.

Initiating faults consist of any perturbation of normal operation, whether caused by internal failures within the reactor systems, errors by operators, or by events outside the reactor system. These latter events may be initiated on-site (Internal Hazards) or off-site (External Hazards).

24.4.2 Fault Identification Based on Logic Tree Analysis

The initiating events to be analysed were initially identified by using logic tree analysis. Then, the lists of identified faults were compared with relevant guidance used by the IAEA and US-DCD [Ref-1, Ref-2] and completeness confirmed by using tools such as Master Logic Diagrams (MLDs) and FMEA, as described in section 24.4.3.

Initially, faults are divided into seven groups – the first five corresponding to faults in the reactor during normal operation, including shut-down; and the last two to other sources of radioactivity (spent fuel and radioactive waste).

(1) Startup

(2) Power Operation

- (3) Hot Shutdown
- (4) Cold Shutdown
- (5) Refuelling outage
- (6) Spent Fuel Storage Pool Cooling Systems
- (7) Radioactive Waste System

The method of identifying initiating events for the reactor by using logic tree analysis is explained below. Figure 24.4.2-1 shows the method of identifying postulated initiating disturbances in the core. Firstly, abnormal states which may lead to damage to nuclear fuel or the reactor coolant pressure boundary, and potentially lead to the release of radioactive materials from the nuclear facility were identified. Next, the causes were identified for each abnormal state and grouped together. Finally, postulated disturbances were identified for each cause. This results in twelve postulated disturbances affecting the reactor for further consideration in the next stage of the identification of DB initiating events. These twelve disturbances are shown in the right hand side of Figure 24.4.2-1.

Figure 24.4.2-2 gives an example of the application of the methodology for identifying initiating events for the UK ABWR that can lead to one of the postulated disturbances in Figure 24.4.2-1 (specifically 'Increase in reactor pressure'). All initiating events have been identified in this way.

Although the initiating events and the possible state of plants involved in them are numerous, initiating events can be grouped according to the types of influence on the nuclear reactor or the safety systems demanded, and bounding faults are chosen for each group of faults. Bounding faults are those that make the greatest demand on the corresponding safety systems or that have the highest unmitigated consequences and their analysis envelopes other faults in the same group.

In Figure 24.4.2-2, for example, "Turbine control valve fast closure" is similar to "Turbine stop valve closure", but "Turbine control valve fast closure" is the more severe in relation to the reactor pressure rise. Therefore, "Turbine control valve fast closure" is chosen as one of the bounding faults requiring transient analysis to evaluate the resulting plant state.

Similarly, "Feedwater controller failure" is bounded by another postulated disturbance, "abnormal change in reactor coolant inventory".

The detailed results of the logic tree analysis are presented in the Topic Report on Fault Assessment [Ref-3].

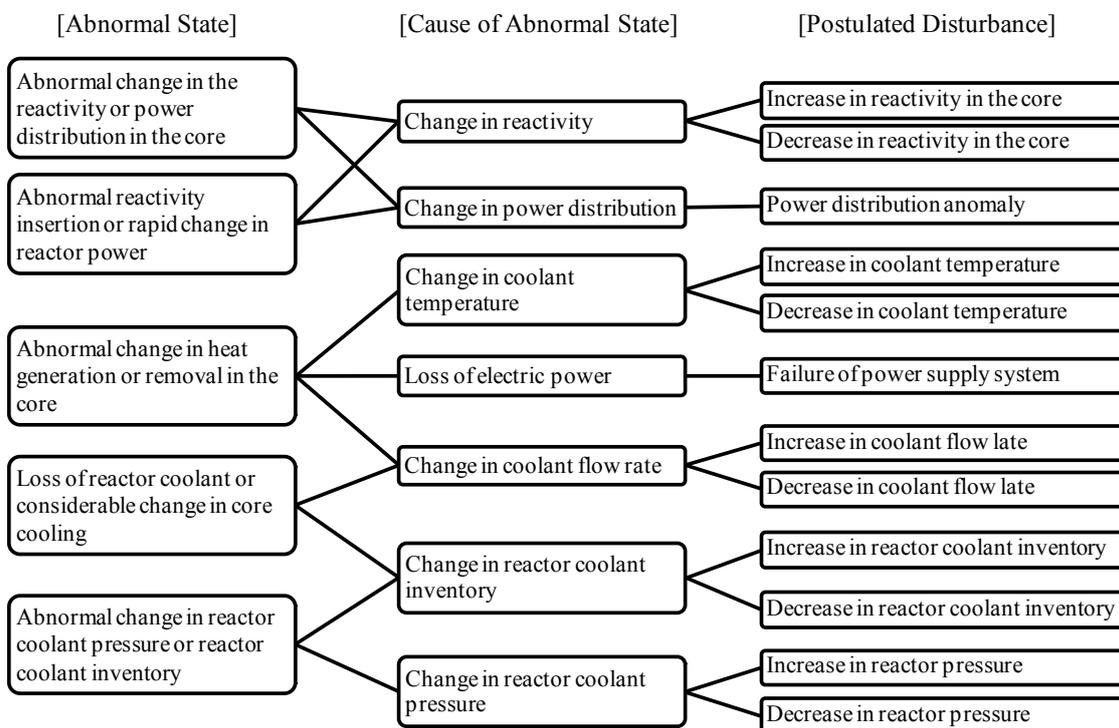


Figure 24.4.2-1: Logic Tree Analysis for Identification of Reactor Postulated Disturbances for UK ABWR

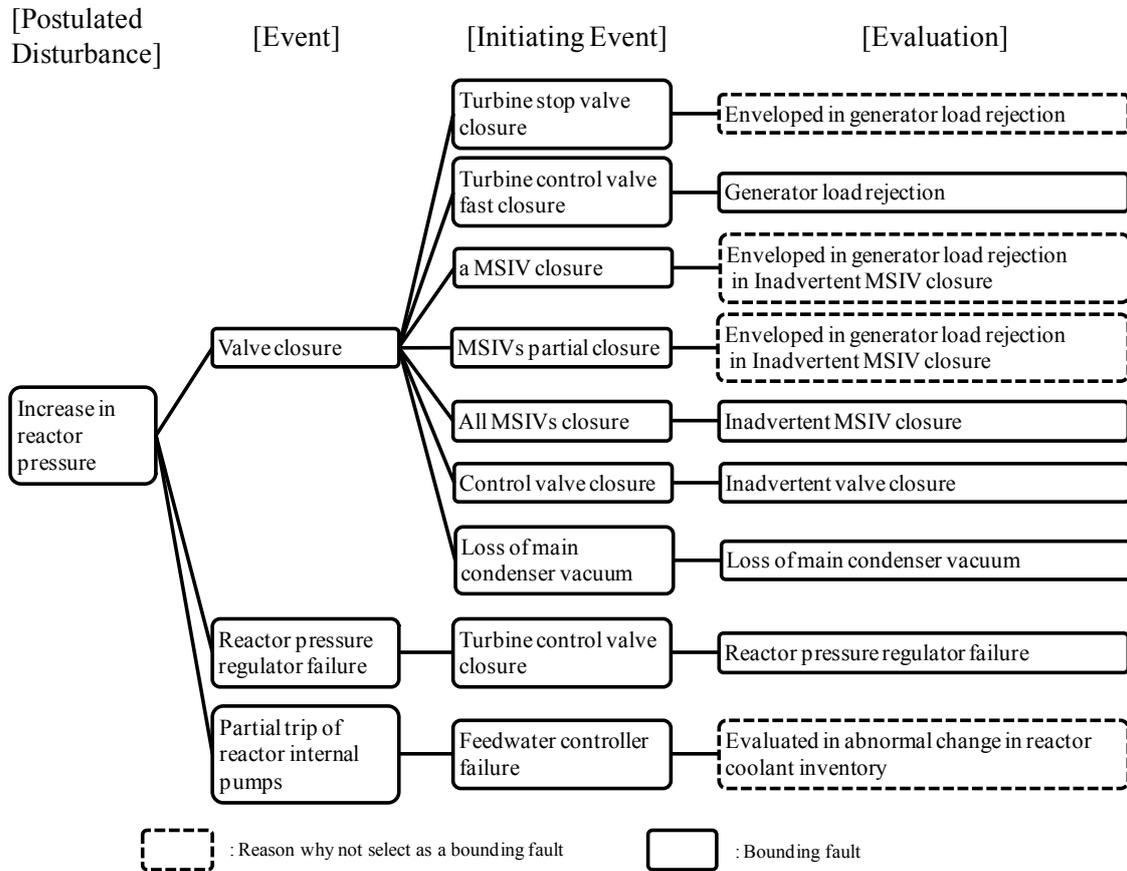


Figure 24.4.2-2: Example of Logic Tree Analysis for Identification of Reactor Initiating Events for UK ABWR

24.4.3 Types of Fault

The purpose of the analysis is to demonstrate the adequacy of the various protection and safety systems in the UK ABWR design. In demonstrating this adequacy, there are a number of considerations and distinctions which are important for the reactor:

(1) Isolation and non-isolation events

Isolation events are events that leave the reactor isolated from the balance of plant systems (turbine, etc.). Non-isolation events may require isolation in addition to other protection measures.

(2) Transients and LOCAs

For the purposes of the DB analysis in this chapter, ‘transients’ are disturbances from normal operation that do not involve failures of the reactor coolant circuit integrity.

Loss of Coolant Accidents (LOCAs) do involve such failures and so are not described as ‘transients’ based on the definition above. LOCAs require reactor coolant to be replaced in addition to other protection measures.

(3) Mode of operation

The mode of operation prior to an initiating event may affect the availability of some protective measures. For example, low pressure injection is not possible when the reactor coolant circuit is at normal operating pressure but requires depressurization in order to operate.

(4) Frequency of the fault

Faults with initiating event frequencies greater than about 1×10^{-5} /y that could, in principle, lead to doses greater than the BSL are defined as Infrequent Design Basis Faults (IF) (see Chapter 5, section 5.5) if their frequency is less than about 1×10^{-3} /y. Events with frequencies greater than about 1×10^{-3} /y are defined as Frequent Design Basis Faults (FF).

All DB faults require the provision of Category A Safety Functions (See Chapter 5, section 5.6) with SSCs of Class 1. Frequent design basis faults also require additional diverse provision of Category A Safety Functions with SSCs of at least Class 2.

24.4.4 Completeness of the List of Initiating Events

24.4.4.1 Benchmark of the List Based on Comparison with IAEA Guidance and US-ABWR DCD

Initiating Events (IEs) identified in the logic tree analysis described in Section 24.3.2 were compared with the IAEA Safety Guide (NS-G-1.2) [Ref-1], and the US-ABWR DCD [Ref-2], and the completeness of the list of IEs was confirmed. As a result, IEs for the UK ABWR are almost the same as those in the IAEA Safety Guide and the US-ABWR DCD. Faults not evaluated are not severe, low probability, almost the same as other faults, are bounded in other faults, or could not occur in operating practice. The complete results of the benchmarking exercise are shown in the Topic Report for Fault Assessment [Ref-3].

24.4.4.2 Completeness of the List for Reactor Faults

A systematic FMEA exercise including a range of spurious failure and common cause initiators has been undertaken to complement the list of reactor IEs identified in the logic tree analysis. As a result of the systematic FMEA exercise, ten additional IEs have been identified in terms of Common Cause Failures (CCFs) to be evaluated in the DBA. These faults are grouped into Common Cause Failures of Control and Instrumentation (C&I) systems, Electrical distribution systems and Essential Services and Support systems. The analysis of these events is described in Section 24.9.3.

24.4.4.3 Completeness of the List for Reactor Faults in Shutdown Modes

Fault groups and initiating events have been identified for reactor faults in shutdown modes using a Master Logic Diagram (MLD). In addition, initiating events in shutdown modes are complemented from the initiating event candidates identified in the shutdown PSA. As a result of these investigations, eighteen additional IEs have been identified to be evaluated in the DBA. The MLD for Shutdown Modes, and the complete results of this assessment are shown in the Topic Report on Fault Assessment [Ref-3] in detail.

24.4.4.4 Completeness of the List for Spent Fuel Pool and Fuel Route Faults

Fault groups and initiating events have been identified for the SFP and Fuel Route using MLDs, analysis of operating procedures, logic tree analysis and FMEA. Also, fault tree analysis has been used for fault identification in the Spent Fuel Interim Storage. As a result of these analyses, twelve additional IEs have been identified to be evaluated in the DBA in addition to SFIS faults. The complete results of this DB assessment are shown in the Topic Report on Fault Assessment for SFP and Fuel Route [Ref-4] in detail. Faults associated with the SFIS are addressed in Chapter 32.

24.4.4.5 Completeness of the List for Non-Reactor Faults

The failure of SSCs not directly related to the reactor that have the potential to result in a person receiving a significant dose of radiation were identified in a systematic FMEA exercise. As a result of this, several tens of additional IEs have been identified to be evaluated as non-reactor faults in the DBA. It is noted that most additional initiating events identified as non-reactor faults are associated with worker dose in the radioactive waste systems. The complete results of the FMEA are shown in the Topic Report on Fault Assessment [Ref-3] in detail.

24.4.5 List of Bounding Faults

The bounding faults are organised by fault type category ((1) to (17)). The bounding faults are listed in Table 24.4-1 which also shows the fault type and applied acceptance criteria. The section of this chapter where the bounding faults are discussed is also given. The number in brackets after the fault description is the reference to the entry for the fault in the Fault Schedule. The fault schedule gives more data concerning the fault – see Section 24.4.6.

Table 24.4-1: List of bounding Faults considered in the DBA

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
24.6 Non-Isolation Events					
24.6.1 Increase in Reactor Pressure					
–	Generator load rejection with bypass (1.1)	FF	Transient	AC-F3, AC-F2, AC-R1, AC-C1	
24.6.1.1	Feedwater controller failure –Maximum demand (1.4)	FF	Transient	AC-F3, AC-F2, AC-R1, AC-C1	Bounding fault for group
–	Reactor pressure regulator failure in the closed direction (1.7)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Inadvertent control valve closure (1.8)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
24.6.2 Decrease in Reactor Coolant Flow Rate					
–	Partial loss of reactor coolant flow(Trip of three Reactor Internal Pumps) (1.2)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
24.6.2.1	Loss of reactor coolant flow (Trip of all reactor internal pumps) (1.3)	FF	Transient	AC-F3, AC-F2, AC-R1, AC-C1	Bounding fault for group
24.6.3 Increase in Reactor Coolant Flow Rate					
24.6.3.1	Recirculation flow control failure (Runout of all reactor internal pumps) (1.5)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Bounding fault for group
24.6.4 Decrease in Reactor Coolant Temperature					
24.6.4.1	Loss of feedwater heating (1.6)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Bounding fault for group

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Inadvertent High Pressure Core Flooder (HPCF) pump start (1.9)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
24.6.5 Reactivity and Power Distribution Anomalies due to Malfunction of Control Rod System or Reactor Protection System (RPS)					
24.6.5.1	Control rod withdrawal error at reactor start-up (4.1)	FF	Reactivity insertion	AC-F6, AC-R1, AC-C1	
24.6.5.2	Control rod withdrawal error at power (4.2)	FF/IF	Reactivity insertion	AC-F1/3, AC-F2, AC-R1/2, AC-C1	
24.6.5.3	Control rod drop (4.3)	IF	Reactivity insertion	AC-F7, AC-R2, AC-C1	
–	Inadvertent reactor scram [Control Rod Drive (CRD) pump trip] (4.4)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Not severe
–	Start-up Range Neutron Monitor (SRNM) or Average Power Range Monitor (APRM) sensor failure (4.5)	IF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Not severe
–	Radiation monitor failure (4.6)	IF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Not severe
24.7 Isolation Events					
24.7.1 Increase in Reactor Pressure					
24.7.1.1	Generator load rejection with failure of all Bypass valves (1.1)	FF	Transient	AC-F3, AC-F2, AC-R1, AC-C1	
–	Inadvertent Main Steam Isolation Valve (MSIV) closure (2.1)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Reactor pressure regulator failure in the open direction (2.2)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Loss of main condenser vacuum (2.3)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Bounding fault for group
24.7.2 Decrease in Reactor Coolant Inventory (RPV Water Level Decrease Events)					
24.7.2.1	Loss of all feedwater flow (3.1)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Bounding fault for group
24.7.3 Loss of Off-site Power (LOOP)					
24.7.3.1	Short term loss of off-site power (2 hours duration) (5.1)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Bounding fault for group
–	Medium term loss of off-site power (24 hours duration) (5.2)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Long term loss of off-site power (168 hours duration) (5.3)	IF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
24.8 Loss of Coolant Events					
24.8.1 Inadvertent Opening of a SRV					
24.8.1	Inadvertent opening of a SRV (6.1)	FF	LOCA	AC-F1, AC-F2, AC-C1, AC-D1, AC-D2	Bounding fault for group
Small LOCA inside Primary Containment					
–	LOCA –RPV bottom drain line break– (7.1)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D3, AC-D4	Bounded by Medium LOCA

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Small line break LOCA (7.2)	FF	LOCA	AC-F1, AC-F2, AC-C1, AC-D1, AC-D2	Bounded by Medium LOCA
2.4.8.2 Medium LOCA inside Primary Containment					
24.8.2.1	LOCA –HPCF line break– (8.1)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	Bounding fault for group
–	LOCA –Low Pressure Flooder (LPFL) line break– (8.2)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	
2.4.8.3 Large LOCA inside Primary Containment					
24.8.3.1	LOCA –Feedwater line break– (9.1)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	
24.8.3.1	LOCA –Main steam line break– (9.2)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	
–	LOCA –Residual Heat Removal (RHR) Outlet line break– (9.3)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	Bounded by LOCA –Feedwater line break–
24.8.4 Other Type of LOCA					
24.8.4.1	LOCA outside primary containment –Main steam line break– (10.1)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	Bounding fault for group
–	LOCA outside primary containment –Reactor Water Clean-up line break– (10.2)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	
–	LOCA outside primary containment –Feedwater line (Reactor Core Isolation Cooling system (RCIC) connected) break– (10.3)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D5, AC-D6	

24. Design Basis Analysis
 24.4 Fault Identification and Grouping and Fault Schedule
 Ver. 0

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
24.8.4.2	Small line break LOCA outside primary containment (10.4)	FF	LOCA	AC-D1, AC-D2	Representative event
24.9 Common Cause and Multiple Failures					
24.9.1 Anticipated Transient without Scram (ATWS)					
–	Generator load rejection with failure of all Bypass valves with Failure to Scram (1.1.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
–	Feedwater Controller Failure at Maximum demand with Failure to Scram (1.4.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
–	Recirculation Flow Controller Failure at Maximum Demand with Failure to Scram (1.5.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
24.9.1.1	Main Steam Isolation Valve Closure with Failure to Scram (2.1.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	Representative event
–	Pressure Regulator Failure Open – Maximum Steam Demand with Failure to Scram (2.2.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
–	Loss of Condenser Vacuum with Failure to Scram (2.3.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
–	Short term Loss of Offsite Power with Failure to Scram (5.1.3)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
–	Pressure Regulator Failure Open – Maximum Steam Demand with Failure to Scram (2.2.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
24.9.1.2	ATWS instability (Not identified separately in the Fault Schedule)	IF	Transient	AC-F4, AC-F5	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
24.9.2 Station Blackout (SBO)					
–	Short term LOOP with CCF of Emergency Diesel Generators (EDGs) (5.1.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D5, AC-D6	
24.9.2.1	Medium term LOOP with CCF of EDGs (5.2.1)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D5, AC-D6	Bounding Fault for group
24.9.3 Common Cause Failures of C&I systems, Electrical distribution systems and Essential Services and Support systems					
24.9.3.2	All Control Rods, electrical drive units, insertion (11.1)	FF	Transient	AC-F1, AC-F2, AC-R1	Representative event
24.9.3.1	Inadvertent opening of all Automatic Depressurisation System (ADS) (Other Safety System Logic and Control systems (SSLCs) are available) (11.2)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D3, AC-D4	Representative event
–	Inadvertent start-up all injection system (11.3)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	
–	Inadvertent opening of all ADS due to spurious failure of Class 1 SSLC (11.4)	IF	LOCA	AC-F4, AC-F5, AC-C1, AC-D3, AC-D4	
–	Inadvertent MSIV closure due to spurious failure of Class 1 SSLC (11.5)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D3, AC-D4	
–	Inadvertent start-up A1 (RHR,HPCF) injection system in shutdown modes (11.6)	IF	Transient	AC-W1, AC-W2, AC-D5, AC-D6	
–	Inadvertent start-up A2 (FLSS) injection system in shutdown modes (11.7)	FF	Transient	AC-W1, AC-W2, AC-D3, AC-D4	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Metal-Clad switchgear (M/C) power supply failure on electrical CCF (11.8)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D3, AC-D4	Bounded by SBO
–	D/C power supply failure on electrical CCF (11.9)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D3, AC-D4	Bounding Fault for group
–	Loss of all Reactor Building Cooling Water (RCW) (11.10)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D3, AC-D4	Bounded by SBO
–	Loss of all Reactor Building Service Water (RSW) (11.11)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D3, AC-D4	Bounded by SBO
–	Loss of all Class 1 Heating Ventilation and Air Conditioning (HVAC) (11.12)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1, AC-D3, AC-D4	Bounded by D/C power supply failure on electrical CCF
24.10 Reactor Faults other than at Power					
24.10.1 Reactor Fault on Partial Power Operation					
–	Generator load rejection (without power load unbalance relay) (1.1.1/12.1)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
24.10.1.1	Generator load rejection on scram bypass power (1.1.2/12.2)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	Representative event
–	Trip of all Reactor Internal Pumps (RIPs) on scram bypass power (1.3.1/12.3)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
24.10.2 Reactor Fault in Shutdown Modes					

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Control rod withdrawal error in shutdown modes (13.1)	FF	Reactivity insertion	AC-F6	Bounded by Control rod withdrawal error at reactor start-up
–	Misloading of fuel bundle during refuelling (13.2)	IF	Reactivity insertion	AC-F1, AC-F2, AC-F7	Not severe
24.10.2.1 .1	Loss of operating RHR with loss of the same division of ECCS (13.3)	FF	Transient	AC-W1, AC-W2, AC-D3, AC-D4	Bounding fault for Loss of decay heat removal events of group
–	Loss of operating RHR due to CCF of Class 1 controller (13.4)	FF	Transient	AC-W1, AC-W2, AC-D3, AC-D4	
–	LOOP (13.5)	FF/IF	Transient	AC-W1, AC-W2	
–	SBO (13.6)	IF	Transient	AC-W1, AC-W2, AC-D5, AC-D6	
–	Draindown due to valve failure within the operating RHR (13.7)	FF/IF	LOCA	AC-W1, AC-W2, AC-D3, AC-D4	
–	LOCA at feedwater line inside Primary Containment Vessel (PCV) (13.8)	IF	LOCA	AC-W1, AC-W2, AC-D5, AC-D6	
24.10.2.2 .1	LOCA at RHR suction line inside PCV (13.9)	IF	LOCA	AC-W1, AC-W2, AC-D5, AC-D6	Bounding fault for LOCA above TAF of group
–	LOCA at LPFL return line inside PCV (13.10)	IF	LOCA	AC-W1, AC-W2, AC-D5, AC-D6	

24. Design Basis Analysis
24.4 Fault Identification and Grouping and Fault Schedule
Ver. 1

NOT PROTECTIVELY MARKED

24.4-15

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	LOCA (mechanical) below TAF (13.11)	IF	LOCA	AC-W1, AC-W2, AC-D5, AC-D6	
–	RPV draindown by Reactor Water Clean-up system (CUW) (13.12)	FF	LOCA	AC-W1, AC-W2, AC-D1, AC-D2	
–	Leakage during Fine Motion Control Rod Drive (FMCRD) inspection (13.13)	FF	LOCA	AC-W1, AC-W2, AC-D1, AC-D2	
24.10.2.2	Leakage during replacement In-core Monitor (ICM) nozzle (13.14)	FF	LOCA	AC-W1, AC-W2, AC-D1, AC-D2	Bounding fault for LOCA below TAF of group
–	Leakage during RIP inspection (13.15)	FF	LOCA	AC-W1, AC-W2, AC-D1, AC-D2	
–	Refuelling Bellows Perforation caused by an Irradiated Fuel Drop (13.16)	IF	LOCA	AC-W1, AC-W2, AC-D3, AC-D4	
–	LOCA at CUW system line outside PCV (13.17)	IF	LOCA	AC-W1, AC-W2, AC-D5, AC-D6	
–	LOCA at RHR system line outside PCV (13.18)	IF	LOCA	AC-W1, AC-W2, AC-D5, AC-D6	
24.11 Non-Reactor Faults					
24.11.1 SFP and Fuel Route Faults					
24.11.1.1	Loss of all Fuel Pool Cooling (FPCs) during SFP gate closed (14.1)	IF	Transient	AC-N1, AC-W2, AC-D3, AC-D4	Representative event
–	LOOP during irradiated fuel or Control Rod (CR) handling between SFP and the core (14.2)	FF/IF	Transient	AC-N1, AC-W2	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	SBO during SFP gate closed (14.3)	IF	Transient	AC-N1, AC-W2, AC-D5, AC-D6	
–	Small leak of SFP (liner clacking or damage from Internal/External hazard) (14.4.1)	IF	Transient	AC-N1, AC-W2, AC-D3, AC-D4	
–	FPC line break (14.4.2)	IF	Transient	AC-N1, AC-W2, AC-D5, AC-D6	
24.11.1.2	Fuel drop into the core during irradiated fuel handling between SFP rack and the core (14.5)	IF	Impact	AC-N1, AC-D3, AC-D4	Representative event
–	Fuel collision during irradiated fuel handling between SFP rack and the core (14.6)	FF	Impact	AC-D3, AC-D4	
–	Drop of heavy equipment into the core (14.7)	IF	Impact	AC-D3, AC-D4	
–	Drop of heavy equipment into SFP (14.8)	IF	Impact	AC-D3, AC-D4	
–	Over-raise of irradiated fuel (14.9)	FF	Radiation Exposure	AC-D1	
–	Over-raise of irradiated equipment (14.10)	FF	Radiation Exposure	AC-D1	
24.11.1.3	Dropped sealed canister/transfer cask from the reactor building crane onto the ground floor (SFIS.3.1)	IF	Impact	AC-D3, AC-D4, AC-C2	Representative event
–	Delays during unsealed canister handling and preparation - Time to boil (including LOOP) (SFIS.1.1)	FF	Transient	AC-D1, AC-D2	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Failure of CCS during preparation / Mis-operation of CCS (SFIS.1.3)	FF	Transient	AC-D1, AC-D2	
–	Drying System temperature control fault/Malfunction of drying device or back filling device (SFIS.1.4)	FF	Transient	AC-D1, AC-D2	
–	Dropped unsealed canister / transfer cask from reactor building crane into the cask pit (SFIS.2.4)	FF	Impact	AC-D1, AC-D2	
24.11.2 Radioactive Waste System Leak or Failure					
24.11.2.1	Off-Gas treatment system failure (15.1)	IF	Radiation Exposure	AC-D5, AC-D6	Representative event
24.11.2.2.1	Liquid Radioactive Waste system leak or failure (15.2)	FF	Radiation Exposure	AC-D1, AC-D2	Representative event
24.11.2.2.2	SS Pipe Rupture (15.3)	FF	Radiation Exposure	AC-D1	Representative event
–	Catastrophic Failure of Powder Resin Storage Tank (15.4)	FF	Radiation Exposure	AC-D1	
–	Spread of containment due to maintenance failure (15.5)	IF	Radiation Exposure	AC-D3	
–	Solid Radioactive Waste system leak or failure	FF	Radiation Exposure	AC-D1	
24.11.3 Other Non-Reactor Faults					
–	Loss of clean-up water function (16.1)	FF	Radiation Exposure	AC-D1	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Radiation dose increase in RCW (16.2)	FF/IF	Radiation Exposure	AC-D1/3, AC-D2/4	
–	Evaporator failure (16.3)	FF	Radiation Exposure	AC-D1, AC-D2	
–	Reactor inner supports or fuel assembly break due to dropped load (16.4)	IF	Impact	AC-D5, AC-D6	
–	CUW Pump Inspection and Maintenance (16.5)	FF	Radiation Exposure	AC-D1	
–	FMCRD Replacement – Overhaul (16.6)	FF	Radiation Exposure	AC-D1	
Internal Hazard					
–	Internal Fire in the Reactor Building (17.1)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Internal Fire in Heat Exchanger Building (17.2)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Internal Fire in Control Building (17.3)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Internal Fire in the Main Control Room (17.4)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Internal Missile in the Main Control Room (17.5)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	

Table 24.4-1: List of bounding Faults considered in the DBA (Continued)

Section	Bounding Fault (Event ID)	FF/IF	Fault type	Acceptance criteria	Notes
–	Turbine Missile (17.6)	IF	LOCA	AC-F4, AC-F5, AC-R2, AC-C1, AC-D5, AC-D6	
External Hazard					
–	Loss of Ultimate Heat Sink (18.1)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	10 ⁻³ /year Earthquake (18.2)	FF	Transient	AC-F1, AC-F2, AC-R1, AC-C1	
–	Design Basis Earthquake (DBE) (18.3)	IF	Transient	AC-F4, AC-F5, AC-R2, AC-C1	

24.4.6 Fault Schedule for UK ABWR

The fault schedule lists all fault groups and the individual bounding faults within the groups. It identifies safety functions relevant to each fault and the SSCs that are claimed to deliver them in the DB assessment, identified from the basic safety design, including diverse delivery of safety functions for frequent design basis faults. The purposes of the fault schedule are the identification of safety functions for each bounding initiating event, the demonstration of design basis adequacy, the establishment of technical specification operational bases and the identification of operator actions needed to satisfy the plant essential protection safety measures.

(1) Essential Protection safety measures

Identify and demonstrate that essential protection safety measures needed to accommodate each design basis fault are available and adequate.

(2) Design Basis Adequacy

Identify and demonstrate that the safety design basis of the various SSCs needed to deliver the plant essential protection measures are appropriate, available and adequate. Each protective measure identifies the specific SSCs performing safety functions. The individual design bases are brought together by Design Basis Analysis (DBA).

(3) Human Reliability Analysis Basis

Identify operator actions needed to successfully deliver the plant essential protective measures as described in Chapter 27.

Table 24.4-2 shows an example of the fault schedule for the UK ABWR. The complete fault schedule for UK ABWR is a combination of the fault schedules presented in the Topic Report on Fault Assessment [Ref-3] and in the Topic Report on Fault Assessment for SFP and Fuel Route [Ref-4]. DBA is performed to justify the complete fault schedule. The results of the DBA are described in Section 24.5.

The fault schedule is the main link between the fault assessment presented in this chapter and the safety functional claims and safety property claims listed in the engineering chapters. In the Fault Schedule, the HLSF provided by SSCs listed under each FSF is given in the brackets after the SSC along with the classification of the SSC and the mode of initiation. So, for example, “RPS scram ‘Turbine control valve fast closure’ (A1, Ω , 1-3)” listed under the FSF “Reactivity control” in Table 24.4-2 for the Generator load rejection fault means that the scram function is classified as A1; is automatically initiated; and provides HLSF 1-3. Similarly, operator actions are identified with the HBSC they provide. The Σ identifies the entry as a human action; the A1 refers to the classification

of the associated SSC; and the 3-1 is the HLSF as before. Appendix A, Table A-3 gives the corresponding Human Based Safety Claims (HSBCs).

In the Fault Schedule the principal Class 1 means of providing HLSFs are shown in bold black type. For frequent faults, the secondary Class 2 means of providing HLSFs are shown in blue italic type. Any means of providing HLSFs by Class 3 systems for defence in depth are shown in green italic type.

The correspondence between SFCs and the fault analysis described in this chapter is shown in Appendix A. The link to corresponding SPCs is shown in Appendix B.

Table 24.4-2: Example of the Fault Schedule for UK ABWR

Initiating Fault / Event ID	Initiating Event (Bounding Fault)		Freq (pry)	Unmitigated Consequence		Operating State	Key Plant Impact (including consequential loss)	Fundamental Safety Functions			Comments
	Bounding Fault	Other Fault		Worker	Public			Reactivity Control	Fuel Cooling	Long-term Heat Removal	
1 Non-isolation event											
1.1	Generator load rejection	• Turbine control valve failure • Turbine trip	FF	> 500 mSv	> 100 mSv	A	Pressure boundary: Intact Off-site power: Supplied MS line: Not isolated Feedwater & Condensate system: Available Support System: Available Turbine control valve fast closure → Reactor Scram & SRV(safety) open → Power/Pressure reduced & PCT decrease → Hot shutdown → Depressurisation & Decay heat removal → Cold shutdown	RPS scram "Turbine control valve fast closure" (A1, Ω, 1-3) <i>SLC "High RPV pressure (+timer)" (1/2, A2, Ω, 1-5)</i> <i>+RPT "High RPV pressure" (A2, Ω, 1-5)</i> <i>+Feedwater Stop High RPV pressure(+timer)" (A2, Ω, 1-5)</i> <i>ARI "High RPV pressure" (A2, Ω, 1-5)</i> <i>+RPT "High RPV pressure" (A2, Ω, 1-5)</i> <i>RPT "Turbine control valve fast closure" (C3, Ω, 1-8)</i> <i>FMCRD Run-in "High RPV pressure" (C3, Ω, 1-5)</i>	RCIC "Low water level 2" /HPCF "Low water level 1.5" (1/3, A1, Ω, 2-1) + SRV -Safety valve function- (A1, Ø, 2-1) <i>Alternative SRV (RDCF) "Low water level 1 (+timer)" (7/7, A2, Ω, 2-2)</i> <i>+ FLSS "Low water level 1 (+timer)" (1/2, A2, Ω, 2-2)</i> <i>Transient ADS "Low water level 1 (+timer)" (7/7, B2, Ω, 2-1)</i> <i>+ LPFL "Low water level 1" (1/3, B2, Ω, 2-1)</i> <i>Feedwater & Condensate system (C3, Ø, 5-10)</i> <i>+ Turbine bypass (C3, Ω, 2-1)</i> <i>+ SRV -Relief valve function- (C3, Ω, 2-1)</i>	SRV-Manual depressurisation-- (2/7, A1, Σ, 3-1) S/P cooling with RHR "High S/P water temperature" (1/3, A1, Ω, 3-1) or LPFL with RHR Hx (1/3, A1, Σ, 3-1)*1 or Shutdown cooling with RHR (1/3, A1, Σ, 3-1)*1 <i>Containment venting (1/2, A2, Σ, 3-2)</i> <i>PCS (C3, Ø, 5-10)</i>	Support systems are described in Attachment 1 *1 : In case of failure of manual operation, long term heat removal can also be triggered automatically by high pressure core injection with S/P cooling or LPFL with heat exchanger.
5 Loss of off-site power											
5.1	Short term Loss of off-site power (Short term ≤ 2hr)	• Loss of auxiliary power	FF	> 500 mSv	> 100 mSv	A	Pressure boundary: Intact Off-site power: Not supplied MS line: Isolated Feedwater & Condensate system: Unavailable Support System: Available LOOP → Turbine Control Valve fast closure → Reactor Scram → Power/Pressure reduced & PCT decrease → ECCS water injection supported by EDG → Hot shutdown → Depressurisation & Decay heat removal → Cold shutdown	RPS scram "Turbine control valve fast closure or Turbine stop valve closure or Low water level 3" (A1, Ω, 1-3) <i>SLC "High RPV pressure or Low water level 2 (+timer)" (1/2, A2, Ω, 1-5)</i> <i>ARI "High RPV pressure or Low water level 2" (A2, Ω, 1-5)</i> <i>MG set (C3, Ø, 1-6)</i> <i>FMCRD Run-in "High RPV pressure or Low water level 2" (C3, Ω, 1-5)</i>	RCIC/HPCF "Low water level 1.5" (1/3, A1, Ω, 2-1) + SRV -Safety valve function- (A1, Ø, 2-1) <i>Alternative SRV (RDCF) "Low water level 1 (+timer)" (7/7, A2, Ω, 2-2)</i> <i>+ FLSS "Low water level 1 (+timer)" (1/2, A2, Ω, 2-2)</i> <i>Transient ADS "Low water level 1 (+timer)" (7/7, B2, Ω, 2-1)</i> <i>+ LPFL "Low water level 1" (1/3, B2, Ω, 2-1)</i> <i>SRV -Relief valve function- (C3, Ω, 2-1)</i>	SRV-Manual depressurisation-- (2/7, A1, Σ, 3-1) S/P cooling with RHR "High S/P water temperature" (1/3, A1, Ω, 3-1) or LPFL with RHR Hx (1/3, A1, Σ, 3-1)*1 or Shutdown cooling with RHR (1/3, A1, Σ, 3-1)*1 <i>Containment venting (1/2, A2, Σ, 3-2)</i>	Support systems are described in Attachment 1 *1 : In case of failure of manual operation, long term heat removal can also be triggered automatically by high pressure core injection with S/P cooling or LPFL with heat exchanger. [AC power supply function] Emergency DG "The signal of low voltage of emergency medium voltage bus" (1/3, A1, Ω, 5-2) <i>B/B Generator "The signal of low voltage of the class 2 emergency bus or Low water level 1 (+ timer)" (1/2, A2, Ω, 5-3)</i> <i>Diverse Additional Generator (1/1, B3, Σ, 5-3)</i> [Confinement/Containment Function] MSIV closure "Low water level 1.5 or Low main condenser vacuum" (1/2, A1, Ω, 4-7) <i>Primary containment (A1, Ø, 4-7)</i> <i>PCIS closure "Low water level or High D/W pressure" (1/2, A1, Ω, 4-7)</i> <i>Secondary containment (B2, Ø, 4-7)</i> <i>R/A HVAC isolation damper closure "Low water level 3" (1/2, B2, Ω, 4-7)</i> <i>SGTS "Low water level 3" (1/2, B2, Ω, 4-7)</i>

DBA claims – Additional Protection Paths - Mitigative systems not included in claim for dose target of NSEDPs (Safety cat/class, Initiation type, HLSF No.) or (Number of necessary systems, Safety cat/class, Initiation type, HLSF No.)
Initiation type: Ω Automatic - Σ Manual - Ø No initiating action required

24.5 Design Basis Analysis for UK ABWR

24.5.1 Introduction

DBA is carried out for the bounding design basis faults to confirm the adequacy of the safety design and the suitability and sufficiency of the safety measures against the dose limits specified in the NSEDPs [Ref-24].

The base set of DBA for the UK ABWR was performed as described in [Ref-5], and this section shows representative analysis results for frequent and infrequent design basis faults. The sequence and progress of each fault is described based on the analysis results. The analysis results confirm that the basic design policies of safety systems and safety related systems on the UK ABWR are adequate in order to meet all relevant acceptance criteria and reduce doses to workers and public SFAIRP.

24.5.2 Basic Policy of Design Basis Analysis

(1) Analysis Scope

In analysing postulated initiating events and the subsequent fault sequences, the initial condition is selected so that it would be the most conservative in the light of acceptance criteria, operating mode, allowable operating conditions and fuel burnup, both during a refuelling cycle and accounting for long-term variations due to refuelling and operating history. In addition, the analysis is performed, in principle, until the event has been recovered and the reactor can reasonably be presumed to be in a cold shutdown state without any problem.

For each fault analysed, a single set of analysis is considered appropriate for use in the assessment against all of the applicable plant limits identified. The small changes in assumptions that would be made to assess against the different plant limits would not affect the calculated results to an extent sufficient to significantly erode the identified margins to the plant limits.

(2) Assumptions for Safety Functions

In the analysis of DB faults, the SSCs that provide the HLSFs are assumed to comply with the generic Safety Property Claims (SPCs) given in Chapter 5 Table 5.3-1. The relevant SPCs are listed in Appendix B of this chapter. In addition, the analysis makes the following assumptions:

- (a) Within the safety functions coping with a design basis initiating event or fault sequence, the claimed A1, A2 or A3 safety systems that are identified in the Fault Schedule and presented in Table 24.3-1 are considered as appropriate in each analysis.

- (b) Correct performance of lower class systems are not assumed where this would alleviate the consequence.
- (c) The single failure criterion is applied to the design basis analysis. A single failure and unavailability due to maintenance or testing are conservatively assumed for A1 SSCs delivering any of the fundamental safety functions, namely, reactivity control, fuel cooling, long term heat removal and containment functions. The single failure taken into account is a random failure of the active components and independent of the initiating event. It is conservatively assumed that a single failure makes an entire division unavailable. For A1 SSCs, it is also assumed that one division is under maintenance or testing if this is allowed by the Tech. Specs associated with the SSC. Redundancy requirements to allow for maintenance and testing and single failures are part of the SPCs discussed in Appendix B. Normally, the assumption in the fault studies presented in this chapter is that only one division of any safety system is available. For A2 SSCs, the single failure criterion is not applied although it is still assumed that one division is unavailable because of maintenance and testing. The single failure criterion is also applied to essential supporting systems [Ref-34].
- (d) For SSCs which have been operating before the event and continue to operate as is after the occurrence of the event, no failure is assumed, in principle. However, for most events, it is assumed that there is a simultaneous loss of off-site power, which would render most Class 3 systems inoperable.
- (e) Regarding the manual operation necessary to be performed by the operator, appropriate and sufficient time for that operation is considered. In any case, it is conservatively assumed that no operator action is taken for a period of 30 minutes following any initiating event.
- (f) For some events, it is assumed that safety systems experience common cause failure (CCF). In these cases, the assumption of CCF is also applied to essential supporting systems [Ref-34].

(3) Model and Parameters Used for Analysis

The models and parameters used for analysis are selected so that the analysis result is conservative. The input parameters used in the analysis are conservative values and bound the allowable operating envelope. The analytical values for some system characteristics, such as SRV delay/stroke time, reactor internal pump coastdown time constant, etc., bound the design specification for that system. All setpoints for the protection system assumed in the analyses are conservative, which includes instrument uncertainty, calibration error and instrument drift. The nominal and allowable values for these setpoints controlled by the Technical Specifications assume that the actual setpoints (including maximum uncertainties, etc.) will not exceed the values that are assumed in the analyses.

The parameters relating to radioactivity chemical behaviour are conservatively determined based on OPEX, experimental data and theoretical study, etc. The following parameters are studied in details [Ref-17]:

- Quantity and speciation of radioactivity released from fuel
- Retention of radionuclides on containment wall surfaces
- Dissolution and scrubbing of radionuclides into the Suppression Pool
- Retention of radionuclides in the Suppression Pool
- Retention of radioactivity in the primary containment
- Retention in the secondary containment
- Rate of leakage of radioactivity from the Reactor Building
- Retention of radioactivity in the main steam line piping
- Retention of radioactivity in the Stand-by Gas Treatment System
- Retention of radioactivity in the Spent Fuel Storage Pool water
- Rate of release of radioactivity from the Liquid Radioactive Waste Tank
- Retention of radioactivity in the Charcoal adsorbers
- Retention of radioactivity in reactor water

(4) Initial Power/Flow Operating Constraints

The operating power/flow map used for the design basis analysis is shown in PCSR Chapter 11, Figure 11.5-11. The analyses basis for most of the system response analyses is 100% thermal power, in some assessments, principally LOCA cases, 102% thermal power is used to ensure conservatism. The allowable core flow range is from 90% to 111% rated flow at rated thermal power. Therefore, initial core flow is set at 90%, 100% or 111% rated flow at 100% or 102% thermal power, whichever is the most conservative.

(5) Dose Assessment Approach

The dose to persons exposed to radioactivity is dependent on many factors including exposure pathways, location of the exposed persons and assumptions regarding their habits and behaviours. For off-site locations, three age groups (infant, child and adult) are considered. These persons are conservatively assumed to reside at, and source their food from, a location along the site boundary (approximately 300 m downwind of the radioactivity release point). The following pathways are assessed:

Off-site

- Internal exposure from inhalation of material in the radioactive cloud
- Internal exposure from the ingestion of radioactive contaminated foodstuffs
- External exposure from the radioactive cloud (cloudshine)
- External exposure from material deposited on the ground or on structures (groundshine)

On-site

- Internal exposure from inhalation of radionuclides dispersed in air
- External exposure from radionuclides dispersed in the air (cloudshine)

The occupancy and food ingestion habits of the exposed persons are based on generic habits data taken from NRPB-W41 [Ref-31]. Full occupancy (i.e. 8760 h/y) and the most conservative indoor occupancy factors for each age group are adopted. The exposed persons are assumed to consume two types of food at higher (97.5 percentile) rates and other foods at average rates, in accordance with the 'top-two' approach.

The assumed breathing rate for each age group is based on average breathing rates published in ICRP 71 [Ref-32], which take age and activity levels into account.

Dose conversion coefficients for internal exposure pathways (inhalation and ingestion) are based on ICRP Publication 119. Dose conversion coefficients for external exposure pathways are taken from FGR12 [Ref-33].

Doses to exposed persons from exposure to airborne radionuclides (via inhalation and cloudshine pathways) were calculated using the RADTRAD computer code [Ref-14]. The doses due to deposited material (for exposures via groundshine and ingestion pathways) were calculated using spreadsheet tools incorporating the integrated radionuclide concentrations in air, soil and food; the dose coefficients for the exposure pathways considered; and the exposure factors associated with the pathways assessed (such as indoor occupancy factors and food consumption rates).

24.5.3 Analysis Codes

Table 24.5-1 lists the computer codes used for the DBA for the UK ABWR. An outline description of each computer code is presented in the following subsections. More detailed descriptions of the computer codes and their validation are described in the relevant reference documents.

Table 24.5-1: Computer Codes used for DBA

Analysis Item	Computer Code
Plant Transient	<ul style="list-style-type: none"> • ODYN [Ref-6] • ISCOR [Ref-7] • TASC [Ref-8]
RWE/CRDA	<ul style="list-style-type: none"> • PANACEA [Ref-9] • TRACG [Ref-10]
LOCA	<ul style="list-style-type: none"> • LAMB [Ref-11] • TASC • SAFER [Ref-12]
PCV	<ul style="list-style-type: none"> • M3CPT [Ref-13] • SHEX [Ref-13]
ATWS	<ul style="list-style-type: none"> • ODYN • ISCOR • TASC • STEMP [Ref-6] • TRACG
SBO	<ul style="list-style-type: none"> • SAFER • SHEX
Dose Evaluation	<ul style="list-style-type: none"> • RADTRAD [Ref-14] • MCNP5 [Ref-19] • ORIGEN2
Safe Shutdown	<ul style="list-style-type: none"> • SHEX
Diverse System Demonstration	<ul style="list-style-type: none"> • SAFER • SHEX

24. Design Basis Analysis
 24.5 Design Basis Analysis for UK ABWR
 Ver. 0

Table 24.5-1: Computer Codes used for DBA (Continued)

Analysis Item	Computer Code
Transient Analysis in Reactor Shutdown modes and SFP	<ul style="list-style-type: none"> • Spread Sheet
Sub-criticality in SFP rack	<ul style="list-style-type: none"> • SCALE6
Number of damaged fuel rods due to drop of heavy equipment	<ul style="list-style-type: none"> • Hand calculation

24.5.3.1 Transient Analysis Codes

(1) ODYN

ODYN is based on the use of a one-dimensional neutron kinetics and thermal-hydraulic simulation of the reactor. ODYN is used to determine the change in key parameters for the event being analysed and provides the transient inputs to enable the change in critical power ratio during the event to be determined.

ODYN requires input from the steady-state nuclear physics methodology and the plant configuration and performance parameters.

(2) TASC

TASC, the single-channel thermal hydraulic analysis code, is for analysing the thermal margin of fuel in the cases of various accidents. The model used in this code is a single channel, which consists of multiple nodes in axial one-dimension. With regard to each node, the heat transfer to coolant is calculated by applying the heat equation for the fuel rods, and the thermal hydraulic behaviour of coolant is calculated by applying the law of conservation of mass, momentum and energy for coolant in the channel.

Input for the code includes the following:

- core data including the geometrical form of the fuel assemblies
- axial power distribution
- initial conditions of the fuel assembly outputs and flow at the channel inlet
- transient data of the fuel assembly outputs, flow at the channel inlet

The code outputs the changes in time of the Critical Power Ratio (CPR) based on the GEXL correlation formula, coolant flow at each node, quality, etc.

(3) PANACEA

PANACEA is used for analysing the reactor core nuclear thermal hydraulic characteristics of a boiling water reactor, and calculates the power distribution and effective multiplication of the entire reactor with a three-dimensional diffusion equation. In addition, based on the calculated power distribution, a thermal evaluation calculation and burn-up calculation are performed. This code is used for a wide range of purposes such as calculations for control rod operation plans, burn-up control, reactor shutdown margin, etc. Convergence calculation is made so as to produce power distributions with void distribution taken into consideration are undertaken.

The major inputs include data representing the reactor core conditions, including the geometrical form of the reactor core, nuclear constants obtained from the nuclear calculation of unit fuel assemblies, data necessary for the thermal hydraulic calculation, control rod patterns, reactor core heat output, etc. Reactor core power distribution, void distribution, burn-up distribution, effective multiplication ratio, etc., are obtained as outputs.

(4) ISCOR

ISCOR, the reactor core thermal hydraulic analysis code, is for analysing the thermal hydraulic characteristics in the reactor core at steady state. It calculates the thermal hydraulic characteristics for each type of fuel assembly in the reactor core and for the entire reactor core.

The distributions of coolant flow to each of the fuel assemblies is obtained by iterative calculations by using the designed power distributions, so that the differences between pressures at the inlet and outlet of the fuel assembly are the same for all of the fuel assemblies, and the thermal hydraulic characteristics including the thermal margin, reactor core pressure loss, etc. are calculated.

The major inputs include data representing the reactor core conditions including the reactor core heat output, core flow, etc., and data related to the power distribution, geometrical form of the fuel assemblies and other data required for the thermal hydraulic calculations. The critical power ratio, pressure losses, void distributions, etc. are obtained as outputs.

(5) TRACG

TRACG is a best estimate transient calculation code for a BWR system. Neutron kinetics calculation for the BWR reactor core, thermal hydraulic calculation for two-phase flow, fuel rod and structure temperature calculation, and control system calculation are coupled with each other to evaluate BWR transient conditions.

TRACG has point, 1-D, and 3-D neutron kinetics models for simulating the feedback effects of moderator density, fuel temperature, boron, and control rod movement on the core power.

The thermal hydraulics of the BWR system is modelled using a three-dimensional model of the reactor vessel and one-dimensional model for other components. A full two fluid representation supplemented by air and boron models is employed for the characterization of two-phase flow, allowing application to transients where thermal non-equilibrium and counter-current flow between phases is significant. TRACG is capable of modelling standard BWR fuels and advanced fuel designs including part length fuel rods and large water rods.

TRACG has a control system model capable of simulating the BWR feedback control system, for example, a pressure control system, a recirculation flow control system, a feedwater control system, etc. In addition to modelling the ABWR, TRACG is also applicable to experimental test facilities constructed from components representative of a BWR. Such experiments have been used in the validation of the code.

(6) May-Witt

May-Witt is used to calculate the decay heat from the spent fuel in the Spent Fuel Storage Pool. May-Witt is the General Electric decay-heat model which considers the contributions from both fission product and heavy-element decay energy.

24.5.3.2 LOCA Analysis Codes

(1) LAMB

The LAMB thermal hydraulic transient analysis code is used for analysing the short-term thermal hydraulic transients in the reactor, and can treat rupture accidents of various primary system piping connected to the reactor pressure vessel. By dividing the RPV and reactor coolant recirculation system into seven nodes and solving a set of equations based on the law of conservation of mass, momentum and energy, this code calculates changes in time in the mass, pressure and enthalpy of coolant in each node, coolant flows between the nodes during the time span from the steady state to several tens of seconds after the occurrence of the accident. For change in the reactor core flow, responses in the flow caused by a coast down of the reactor coolant recirculation pumps from immediately after the rupture can be calculated.

The major inputs include initial conditions such as reactor power, reactor core flow, etc., geometrical form and various hydraulic quantities of the reactor, fuel assembly and reactor core-related data, plant transient characteristic parameters, recirculation pump characteristics, position and area of the assumed rupture, etc. Reactor pressure used for analysing the critical power transient of the fuel rods during the LOCA, change in time in reactor core flow and reactor core inlet enthalpy, flow of bleed from the rupture opening, etc. are obtained as outputs.

(2) TASC

See Section 24.5.3.1 (2).

(3) SAFER

The SAFER thermal hydraulic transient analysis code is for analysing the long-term thermal hydraulic transient in the reactor, and can treat rupture accidents of various primary-system piping connected to the reactor pressure vessel and loss of reactor coolant flow. This code, with the interior of the reactor vessel divided into nine nodes, calculates changes in the reactor pressure and water level of each node. In addition, by inputting the performance characteristics of various Emergency Core Cooling Systems, this code can evaluate the performance of the systems. In evaluating the in-core coolant quantity, the phenomenon that coolant falls to the plenum at the bottom of the core caused by the gas-liquid Counter Current Flow Limitation phenomenon (CCFL) at the upper tie plate, core inlet orifice, etc. and the localization of a subcooled area at the upper part of the core (CCFL breakdown) can be considered.

In addition, this code performs temperature calculations for fuel pellets, fuel cladding and channel boxes, etc. with regard to the average-power fuel assemblies and high-power fuel assemblies. In performing the temperature calculation for fuel cladding, the heat transfer coefficient reflecting the cooling state of the tube, radiation between the fuel rods, and radiation of the fuel rods and channel box can be considered.

In addition, the chemical reaction of the fuel cladding with cooling water or steam (zirconium-water reaction) is calculated by using the Baker-Just formula to obtain the oxidized quantity of the surface. Further, by calculating the pressure inside the fuel rods, the existence of any bulge and / or rupture in the fuel cladding is evaluated. In the case that rupture has occurred, the zirconium-water reaction occurring inside the fuel cladding is also considered.

The major inputs include initial conditions including the reactor power, reactor pressure, etc., the geometrical form and various hydraulic quantities of the reactor, data related to the fuel assemblies and reactor core, plant transient characteristic parameters, characteristics of the ECCS, position and area of the assumed rupture, etc. The reactor pressure, reactor water level, the highest fuel cladding temperature, oxidized quantity of fuel cladding, etc. are obtained as outputs.

24.5.3.3 PCV Analysis Codes**(1) M3CPT**

This short-term containment pressure response analysis code is for analysing changes in the pressure and temperature inside the primary containment during the period of a coolant blowdown immediately after a LOCA. By dividing the primary containment into two nodes representing the

drywell and suppression chamber and solving equations based on the law of conservation of mass and energy, the dynamic equation and the state equation, this code calculates the pressure and temperature inside the containment. Conservatively, the exchange of heat with the instrumentation inside the containment is not considered.

The major inputs include initial conditions including the pressure, temperature, humidity at each part inside the containment, free space area, flow-path area and flow-path resistance, and mass flow and energy discharge quantity from the primary cooling system. Changes over time of the pressure and temperature inside the primary containment are obtained as outputs.

(2) SHEX

This long-term containment pressure response analysis code is for analysing changes in the pressure and temperature inside the primary containment during a long period when the primary containment spray cooling system is in operation after the period of a coolant blowdown after a LOCA. By dividing the containment into two nodes representing the drywell and suppression chamber and solving equations based on the law of conservation of mass and energy, the dynamic equation and the state equation, this code calculates the pressure and temperature inside the containment. Also, an ECCS model, containment spray model and heat exchanger model are incorporated in this code.

The major inputs include the ECCS flow, containment spray flow, heat exchanger model capacity, seawater temperature, etc. in addition to the initial conditions including the pressure, temperature, humidity at each part inside the containment, free space area, flow-path area and flow-path resistance, and mass flow and energy discharge quantity from the primary cooling system. Changes over time in the pressure and temperature inside the primary containment are obtained as outputs.

24.5.3.4 Dose evaluation Code**(1) RADTRAD**

RADTRAD stands for a simplified model for RADionuclide Transport and Removal And Dose estimation. The RADTRAD code uses a combination of tables and numerical models of source term reduction phenomena to determine the time-dependent dose at specified locations for a given accident scenario. It also provides the inventory, decay chain, and dose conversion factor tables needed for the dose calculation. The RADTRAD code can be used to assess occupational radiation exposures, typically in the control room, to estimate site boundary doses, and to estimate dose attenuation due to modification of a model or accident sequence.

(2) MCNP

MCNP is a general-purpose Monte Carlo N-Particle code that can be used for neutron, photon (gamma), electron, or coupled neutron/photon/electron transport calculations. The code is capable of

modelling an arbitrary three-dimensional configuration of materials in geometric cells bounded by first- and second-degree surfaces and fourth-degree elliptical tori. For photons, the code accounts for incoherent and coherent scattering, the possibility of fluorescent emission after photoelectric absorption, and absorption in electron-positron pair production. Important standard features include a flexible general source definition capability; ability to generate and re-use surface sources; geometry and results tally plotters; variance reduction techniques; a flexible tally structure and an extensive collection of cross-section data. It is estimated that the number of MCNP users over its release history is more than ten thousand. MCNP is the Radiation Safety Information Computational Center's (RSICC's) most widely requested and distributed computer code and it has been used across the UK nuclear industry as a standard code for shielding assessments.

(3) ORIGEN2

ORIGEN2 is used for calculating the source strength of radioactive sources. This code is for calculating the buildup, decay, and processing of radioactive materials. ORIGEN2 is a revised version of ORIGEN and incorporates updates of the reactor models, cross sections, fission product yields, decay data, and decay photon data, as well as the source code.

24.6 Analysis Results and Fault-based View – Non-Isolation Events

Non-isolation events are transients where the reactor remains connected to the turbine, condensate and feedwater systems. Non-isolation events fall into five groups of transients:

- Increase in reactor pressure – see Section 24.6.1
- Decrease in reactor coolant flow rate – see Section 24.6.2
- Increase in reactor coolant flow rate – see Section 24.6.3
- Decrease in coolant temperature – see Section 24.6.4
- Reactivity and power distribution anomalies due to malfunction of control rod system or RPS – see Section 24.6.5

Table 24.6-1 shows the HLSFs claimed in the analysis of non-isolation events and the Class 1 systems that provide them.

Table 24.6-1: Provision of HLSFs by Class 1 systems for Non-Isolation Events

HLSF	System	PCSR Ref	Notes
1-3 Emergency shutdown of the reactor	CRD	11.5.2, 12.4.3.1	The corresponding setpoints are shown in Table 24.6-3 and performance is shown in Table 24.6-4.
2-1 Functions to cool reactor core	RCIC HPCF SRV	13.4 13.4 12.3.5.2	
3-1 Functions to remove residual heat after shutdown	SRV	12.3.5.2	SRV depressurises reactor so that RHR can function. Heat rejected to RCW and RSW
	RHR	12.3.5.4	
	SSLC	14.6.2.1	SSLC provides the functions to control SSCs related to SRV and RHR.
4-2 Functions to prevent overpressure within the reactor coolant pressure boundary	SRV	12.3.5.2	Safety valve function of SRVs

**Table 24.6-1: Provision of HLSFs by Class 1 systems for Non-Isolation Events
(Continued)**

HLSF	System	PCSR Ref	Notes
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SSLC	14.6.2.1	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system.
5-2 Supporting functions especially important to safety	Class 1 EPS	15.3	Class 1 EPS supplies power to Class 1 SSCs.
	RCW/RSW	16.3.2	RCW/RSW are essential systems for supporting HPCF, RHR and Class 1 HVAC operations.
	UHS	16.3.1	UHS provides sufficient cooling water to the RSW.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 1 HVAC	16.5	Class 1 HVAC ensures the adequate environmental parameters for Class 1 SSCs are maintained.
	HECW	16.3.5.1	HECW provides chilled water for Class 1 HVAC.

Major Plant Specifications related to Setpoints of Safety Systems and other to other items are shown in Table 24.6-3 and Table 24.6-4.

In this section, the analyses presented, assume only the above Class 1 safety systems are available and operate, that is, correct performance of lower class systems such as the recirculation pump trip and the turbine bypass valves are not assumed where this would alleviate the consequences.

Many of the events considered in this section are frequent faults and require diverse provision of the above HLSFs. The demonstration that the faults can be protected by Class 2 SSCs is given in Section 24.12.

The analyses of four representative events of the nine non-isolation events are presented in this section of the PCSR. The analysis conditions are shown in Table 24.6-2. The analyses of the other events are described in the Topic Report on DBA [Ref-5] and these results comply with all acceptance criteria.

Table 24.6-2: Analysis Conditions

Item	Analysis Conditions	Note
Reactor thermal power	3926 MW	
Fuel type	10 × 10 Fuel (GE 14)	
Core flow	52200 t/h 47000 t/h 58000 t/h	Rated core flow 90% core flow 111% core flow Initial flow condition is set to be the most severe condition among the above three core flow.
Reactor dome pressure	7.07 MPa[gauge]	At rated reactor power
Steam flow	7640 t/h	Rated flow
Feedwater temperature	216 °C	At rated reactor power
Water level	Normal operating water level	

Table 24.6-3: Major Plant Specifications Related to Setpoints of Safety Systems

Item	Analysis Conditions	Note
High reactor pressure scram	7.62 MPa [gauge]	
Low reactor water level scram (Level 3)	+0.57 m from the bottom of separator skirt	The bottom of the separator skirt is 1.19 m from the normal water level.
High neutron flux scram in terms of neutron flux	125%	
High APRM simulated thermal power	115%	
Main steam isolation valve closure scram	85% stroke position	100% as full open
Turbine main steam stop valve closure scram	85% stroke position	100% as full open

*The 2 out of 4 logic is applied for Class 1 safety systems, as described in Chapter 14. Therefore the system maintains the safety functions even when considering single failure and maintenance.

Table 24.6-4: Major Plant Specifications Related to Other Items

Item	Analysis Conditions	Note
Main steam isolation valve closure time	3 s	
Turbine steam control valve closure time	0.15 s	A full stroke closure time from fully open to fully closed is 0.15 s.
Scram insertion time	1.71 s at 60% of full stroke 3.70 s at 100% of full stroke	The setpoints of the scram insertion time at the rated pressure are 1.44 seconds or less at 60% insertion of full stroke and 2.80 seconds or less at 100% insertion of full stroke. However, in analysing abnormal operational transients, 1.71 seconds at 60% insertion and 3.70 seconds at 100% insertion are used. The dependence of the control rod drive system on the reactor pressure was taken into consideration in the specification of these values.
Reactor high water level (turbine trip) (Level 8)	+1.73 m from the bottom of separator skirt	This function is assumed if it is relevant to the fault.
Safety Relief Valve setpoints (Safety function)	1st stage : 8.17 MPa [gauge] 2 valves 2nd stage : 8.24 MPa [gauge] 4 valves 3rd stage : 8.31 MPa [gauge] 4 valves 4th stage : 8.38 MPa [gauge] 3 valves 5th stage : 8.45 MPa [gauge] 3 valves	Analysis conditions are 3% larger than nominal setpoints.

Limits and Conditions for Operation

The future licensee shall ensure that, during normal power operation, the following plant conditions are maintained:

- Reactor power shall not exceed 100% of rated power.
- The core flow shall be between 90% and 111% of rated core flow
- The reactor dome pressure shall not exceed 7.17 MPa[gauge]
- Water level is above the low reactor water level scram point.

The future licensee shall ensure that, during normal power operation, one or more divisions of the following systems are operational even if one division is unavailable due to testing or maintenance and another division is unavailable due to a single failure:

- RCIC and HPCF treated as one system
- RHR
- SSLC
- Class 1 EPS
- RCW
- RSW
- UHS
- Class 1 HVAC
- HECW

The future licensee shall ensure that, during normal power operation, the following SSCs are operational:

- CRD
- SRV

24.6.1 Increase in Reactor Pressure

24.6.1.1 Feedwater Controller Failure – Maximum Demand

Fault Schedule Ref: 1.4

(1) Description of Fault

Feedwater controller failure –maximum demand is postulated on the basis of a failure of the control system which directly causes an increase in coolant inventory by increasing the feedwater flow by causing all feedwater pumps to run out to their maximum capacity (136% rated flow). An additional absolute 5% is added to the runout flow as a conservative measure to cover uncertainties.

This event bounds the following events:

- Generator load rejection with bypass (Fault Schedule Ref: 1.1)
- Reactor pressure regulator failure in the closed direction (Fault Schedule Ref: 1.7)
- Inadvertent control valve closure (Fault Schedule Ref: 1.8)

Feedwater controller failure – maximum demand is the bounding event as it is the limiting event for CPR, core average surface heat flux, and vessel bottom pressure.

This fault is assumed to be a frequent fault because it is caused by failure of a Class 3 controller.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the following protections against the fault:

- (i) L8 trip of the turbine and feedwater pumps (Class 3)
- (ii) Reactor scram (Class 1) and trip of 4 RIPs (Class 3) initiated by MSV closure
- (iii) Opening of the turbine bypass valves (Class 3)
- (iv) Opening of the SRV (Relief valve function) (Class 3)

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (ix) below. Further details of the analysis conditions are described in A.5.1.1.4 in the Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2.
- (ii) The feedwater flow is conservatively assumed instantly to reach 141% of the rated flow
- (iii) The initial core flow is assumed to be 111%, which gives the most severe result in sensitivity analysis.
- (iv) This analysis conservatively represents the reactor water level high (Level 8) turbine trip function
- (v) The RIP trip function is not assumed.
- (vi) The operating mode of the Recirculation Flow Control (RFC) (Class 3) is assumed to be manual (frozen).
- (vii) The turbine Electrohydraulic Control system (EHC Class 3) is assumed to be frozen, which maximises the pressure increase caused by the power increase.
- (viii) The Feedwater Control system (FDWC) (Class 3) is assumed to be failed.

- (ix) One division of each of the Class 1 safety systems listed in Table 24.6-1 is assumed to be operational in compliance with assumptions on maintenance and testing and the single failure criterion.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is a frequent fault, the relevant ones are:

- AC-F3: The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning/creep rupture (perforation) temperature, so as to preclude cladding failure.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

Increased feedwater raises the reactor vessel water level and subsequently the reactor pressure rises due to reducing gaseous volume in the vessel. In addition, increased feedwater leads to an increase of core subcooling, and, as a consequence, the reactor power increases. Since these increases are gradual, the situation will settle without reaching the acceptance criteria in spite of the water level

rise. Therefore, the Level 8 turbine trip function is assumed. With this function, the turbine and the turbine driven feedwater pump trip, the Main Steam Valves (MSVs) close and the reactor scrams. The MSV closure brings a large vessel pressure rise and a reactor power spike, however, the vessel pressure is mitigated by operation of the SRVs (safety function). The peak neutron flux reaches 288% of its rated value and the Minimum CPR (MCPR) falls below the safety limit value of 1.06. However, the maximum fuel cladding temperature is limited to about 734 °C.

(d) Analysis Results

The results of the Feedwater controller failure – maximum demand events are shown in Table 24.6-5 and Figure 24.6.4-1.

In the analysis, the MCPR is below the safety limit MCPR value but the maximum fuel cladding temperature is below the limiting value of 800 °C. Therefore the acceptance criteria described above are met as shown below:

- The calculated maximum fuel cladding temperature during this event is about 734 °C and does not exceed 800 °C. In addition, ballooning rupture occurs in none of the fuel rods. (AC-F3 met)
- The peak surface heat flux of the fuel cladding is approx. 128% and does not exceed the thermal over-power (TOP) acceptance criterion of 138%. (AC-F2 met with some margin)
- The peak pressure on the reactor coolant pressure boundary is 8.77 MPa [gauge] and it does not exceed the acceptance criterion value of 9.48 MPa [gauge] (110% of the maximum allowable working pressure). (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not exceed the maximum allowable working pressure since the enthalpy released to the suppression pool via the SRVs is low enough to be removed by the heat removal systems such as the Residual Heat Removal System. (AC-C1 met with significant margin)

(4) Discussion and Conclusions

Although not formally claimed in the design basis, there are a number of Class 3 SSCs providing the HLSFs claimed in this analysis in addition to the Class 1 SSCs in Table 24.6-1. Table 24.6-5 shows the resulting system parameters if these systems function correctly. It is noted that if correct performance of lower class systems, that is, the RIP trip and the SRV (Relief valve) and the Turbine Bypass Valves (TBVs) is assumed, the transient behaviour of this event is milder, and therefore, in the case of the Operating Limit Minimum CPR (OLMCPR) value of 1.28 or more, the MCPR is greater than 1.10 and remains above the safety limit MCPR (1.06) as shown in Table 24.6-5.

Because MCPR remains above the safety limit, fuel criteria are not challenged. Figure 24.6.4-1 shows that RPV pressure remains below the relevant limit of 110% of the maximum allowable working pressure (9.48MPa) (AC-R1). As there is no failure of any barrier, there is no release of radioactive material.

Therefore, all the DBA acceptance criteria are met for this event and there are no radiological releases and no exposure of workers or the public.

Furthermore, Class 3 SSCs provide defence in depth and contribute to the claim that the risks from this event are ALARP.

24.6.2 Decrease in Reactor Coolant Flow Rate

24.6.2.1 Trip of All RIPs

Fault Schedule Ref: 1.3

(1) Description of Fault

Though the RIP power supply system has measures to prevent simultaneous trip of all RIPs and eliminate the cause of the event as far as possible, this event is assumed to trip all RIPs simultaneously during reactor power operation on account of failure of the buses or some other cause, such as common cause failure of the control system.

In such a case, the core flow will decrease rapidly, the core cooling ability will drop and the fuel temperature may rise.

This event bounds the following events:

- Partial loss of reactor coolant flow (Fault Schedule Ref: 1.2)
- Loss of reactor coolant flow (Fault Schedule Ref: 1.3)

Among these events, the limiting event for CPR and the Peak Cladding Temperature (PCT) is Trip of All RIPs. The maximum core average surface heat flux and the maximum vessel bottom pressure are not severe for these events.

The fault is assumed to be a frequent fault as the dominant cause is the failure of a Class 3 controller.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the reactor scram initiated by rapid core flow coastdown (Class 1), which is same as the analysis shown in this section.

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (ix) below. Further details of the analysis conditions are described in A.5.1.1.3 in Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2
- (ii) It is assumed that the power supplies of all RIPs are simultaneously lost.

- (iii) The designed time over which the speed halves from the speed corresponding to the rated core flow of the RIPs and the driving motors is approx. 0.7 seconds. However, a 10% smaller time (0.62 seconds) is used in this analysis in order to give more conservative results.
- (iv) The nuclear conditions for the Beginning of Cycle (BOC) are used to provide conservative analysis results.
- (v) The initial core flow is assumed to be 90%, which gave the most severe result in sensitivity analysis.
- (vi) The RFC (Class 3) does not affect the event since all RIPs are lost.
- (vii) The EHC (Class 3) is assumed to be working.
- (viii) The FDWC (Class 3) is assumed to be working.
- (ix) One division of each of the Class 1 safety systems listed in Table 24.6-1 is assumed to be operational in compliance with assumptions on maintenance and the single failure criterion.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F3: The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning/creep rupture (perforation) temperature, so as to preclude cladding failure.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

When all of the RIPs trip concurrently, the core flow rapidly reduces, the voids increase, and negative reactivity is added into the core. Approximately 2 seconds later reactor scram is initiated, on low core flow. Consequently, neutron and surface heat fluxes will not exceed their initial values. Due to the rapid reduction in the flow rate, MCPR falls below 1.06 during the transient. With the boiling transition, the coefficient of heat transfer from the fuel cladding to the coolant becomes small, and the fuel clad temperature increases. However, the temperature increase stops after a short time

because the reactor is scrammed. The peak cladding temperature during this event is less than 500 °C.

(d) Analysis Results

The results of the Trip of All RIPs are shown in Table 24.6-6 and Figure 24.6.4-2.

The MCPR is below the safety limit MCPR value, but the peak fuel cladding temperature is less than 500 °C and so does not exceed 800 °C. In addition, no ballooning rupture occurs in any of the fuel rods.

- The peak surface heat flux of the fuel cladding does not exceed the initial value. (AC-F3 and AC-F2 met)
- The peak pressure on the reactor coolant pressure boundary is 7.36 MPa [gauge] and so it below the acceptance criterion 9.48 MPa [gauge]. (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not change since no SRVs open in this event. (AC-C1 met with significant margin)

Therefore the acceptance criteria described above are met.

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met for this event. As a result, there are no radiological releases and no exposure of workers or the public.

Whilst the MCPR is below the safety limit MCPR, there is significant margin before the fuel acceptance criteria would be threatened. The same applies to the reactor pressure boundary acceptance criterion.

The margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

24.6.3 Increase in Reactor Coolant Flow Rate

24.6.3.1 Recirculation Flow Control Failure

Fault Schedule Ref: 1.5

(1) Description of Fault

The Recirculation Flow Controller (RFC) controls all ten reactor RIPs at the same speed. Multiple failures in the control system etc. might cause the RFC to erroneously issue a maximum demand to all RIPs. The fault does not bound any other faults.

The fault is assumed to be a frequent fault as the dominant cause is the failure of a Class 3 controller.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the following protections against the fault:

- (i) Reactor scram initiated by neutron flux signal high (Class 1)
- (ii) L3 trip of 4 RIPs (Class 2)

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (viii) below. Further details of the analysis conditions are described in A.5.1.1.5 in Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2.
- (ii) The severest transient is assumed to occur when the speed increase signals are sent to all RIPs because of malfunction of the controller.
- (iii) The speed change rate is limited to $\pm 5\%/s$ for RIPs by the limiter in the main controller.
- (iv) The initial core flow is assumed to be 111%, which gave the most severe result in sensitivity analysis.
- (v) The RFC (Class 3) is failed in the definition of this fault.
- (vi) The EHC (Class 3) is assumed to be working.
- (vii) The FDWC (Class 3) is assumed to be working.
- (viii) One division of each of the Class 1 safety systems listed in Table 24.6-1 is assumed to be operational in compliance with assumptions on maintenance and the single failure criterion.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F1: The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

As the core flow increases, the voids decrease and neutron flux increases. As a result, the power also increases, however, the surface heat flux increases slower than the core flow on account of the fuel heat transfer time constant. Neutron flux continues increasing, until it reaches the high neutron flux scram setpoint and the situation terminates. The high neutron flux scram is achieved in approximately 2.9 seconds, the peak neutron flux reaches approximately 126% of the rated value and the peak surface heat flux reaches approximately 110% of the rated value. The change (reduction) in critical power ratio (Δ CPR) for this event is 0.07. The reactor coolant pressure boundary does not exceed approx. 7.45 MPa [gauge].

(d) Analysis Results

The results of the Recirculation Flow Control failure are shown in Table 24.6-7 and Figure 24.6.4-3.

In summary:

- In the case of an OLMCPR value of 1.28 or more, the MCPR is greater than 1.21, and so remains above the safety limit MCPR (1.06). (AC-F1 met)
- The peak surface heat flux of the fuel cladding is approximately 110%, and so does not exceed the acceptance criterion 138%. (AC-F2 met with some margin)
- The peak pressure on the reactor coolant pressure boundary is 7.45 MPa [gauge], and so it does not exceed the acceptance criterion 9.48 MPa [gauge] (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not change since no SRVs open in this event. (AC-C1 met with significant margin)

The acceptance criteria described above are met.

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met for this event. As a result, there are no radiological releases and no exposure of workers or the public.

Because the MCPR is below the safety limit MCPR, there is significant margin before the fuel acceptance criteria would be threatened. The same applies to the reactor pressure boundary acceptance criterion.

The margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

24.6.4 Decrease in Reactor Coolant Temperature

24.6.4.1 Loss of Feedwater Heating

Fault Schedule Ref: 1.6

(1) Description of Fault

During power operation of the reactor, the feedwater temperature drops gradually as a result of a loss of steam for the feedwater heaters. For this reason, the core inlet is subcooled and the reactor power increases.

This event bounds the Inadvertent HPCF pump start event (Fault Schedule Ref: 1.9).

Loss of feedwater heating is the limiting event for CPR and the maximum core average surface heat flux. The maximum vessel bottom pressure is not severe for these two events.

The fault is assumed to be a frequent fault as the dominant cause is the failure of a Class 3 system.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the reactor scram initiated by thermal heat flux high signal (Class 1), which is same as the analysis shown in this section.

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (viii) below. Further details of the analysis conditions are described in A.5.1.1.8 in Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2.
- (ii) It is assumed that the feedwater temperature will drop by 55.6 °C. The time delay between the feedwater heaters and the feedwater spargers is ignored.
- (iii) The initial core flow is assumed to be 111%, which gave the most severe result in sensitivity analysis.
- (iv) The nuclear conditions for the beginning of cycle (BOC) are used to provide conservative analysis
- (v) Operating mode of the RFC (Class 3) is assumed manual (frozen).
- (vi) The EHC (Class 3) is assumed frozen.

- (vii) The FDWC (Class 3) is assumed working.
- (viii) One division of each of the Class 1 safety systems listed in Table 24.6-1 is assumed to be operational in compliance with assumptions on maintenance and the single failure criterion.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F1: The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

As a result of the loss of feedwater heating, the core inlet subcooling increases and the reactor power rises. The neutron flux increases to approximately 118% of the rated value because of the increase of the inlet subcooling. The surface heat flux also increases to approximately 115% of the rated value, the high APRM simulated thermal power scram signal is output, and reactor scram occurs at approximately 31 seconds. The Δ CPR for this event is 0.17.

(d) Analysis Results

The results of the Loss of feedwater heating fault are shown in Table 24.6-8 and Figure 24.6.4-4.

The results are compared with the acceptance criteria described above as shown below:

- In case of an OLMCPR value of 1.28 or more, the MCPR is greater than 1.11, and so remains above the safety limit MCPR (1.06). (AC-F1 met)
- The peak surface heat flux of the fuel cladding is approx. 115%, and so does not exceed the acceptance criterion 138%. (AC-F2 met with some margin)
- The peak pressure on the reactor coolant pressure boundary is 7.52 MPa [gauge], and so it does not exceed the acceptance criterion 9.48 MPa [gauge]. (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not change since no SRVs open in this

event. (AC-C1 met with significant margin)

(4) Discussion and Conclusions

The above results demonstrate that all the DBA acceptance criteria are met for this event. As a result, there are no radiological releases and no exposure of workers or the public.

Because the MCPR is below the safety limit MCPR, there is significant margin before the fuel acceptance criteria would be threatened. The same applies to the reactor pressure boundary acceptance criterion.

The margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

Table 24.6-5: Results Summary for Feedwater Controller Failure – Maximum demand

(Event Leading to Increase in Reactor Pressure)

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR	PCT (°C)
Figure 24.6.4-1	288	8.77	128	> 0.22	734
(Case of correct performance of lower class system assumed)	167	8.10	109	0.18	N/A

*NBR: Nuclear Boiler Rated

Table 24.6-6: Results Summary for Trip of All RIPs

(Events Leading to Decrease in Core Flow)

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR	PCT (°C)
Figure 24.6.4-2	100	7.36	100	> 0.22	< 500

**Table 24.6-7: Results Summary for Recirculation Flow Control Failure
(Event Leading to Increase in Core Flow)**

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR
Figure 24.6.4-3	126	7.45	110	0.07

**Table 24.6-8: Results Summary for Loss of Feedwater Heating
(Event Leading to Decrease in Reactor Coolant Temperature)**

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR
Figure 24.6.4-4	118	7.52	115	0.17

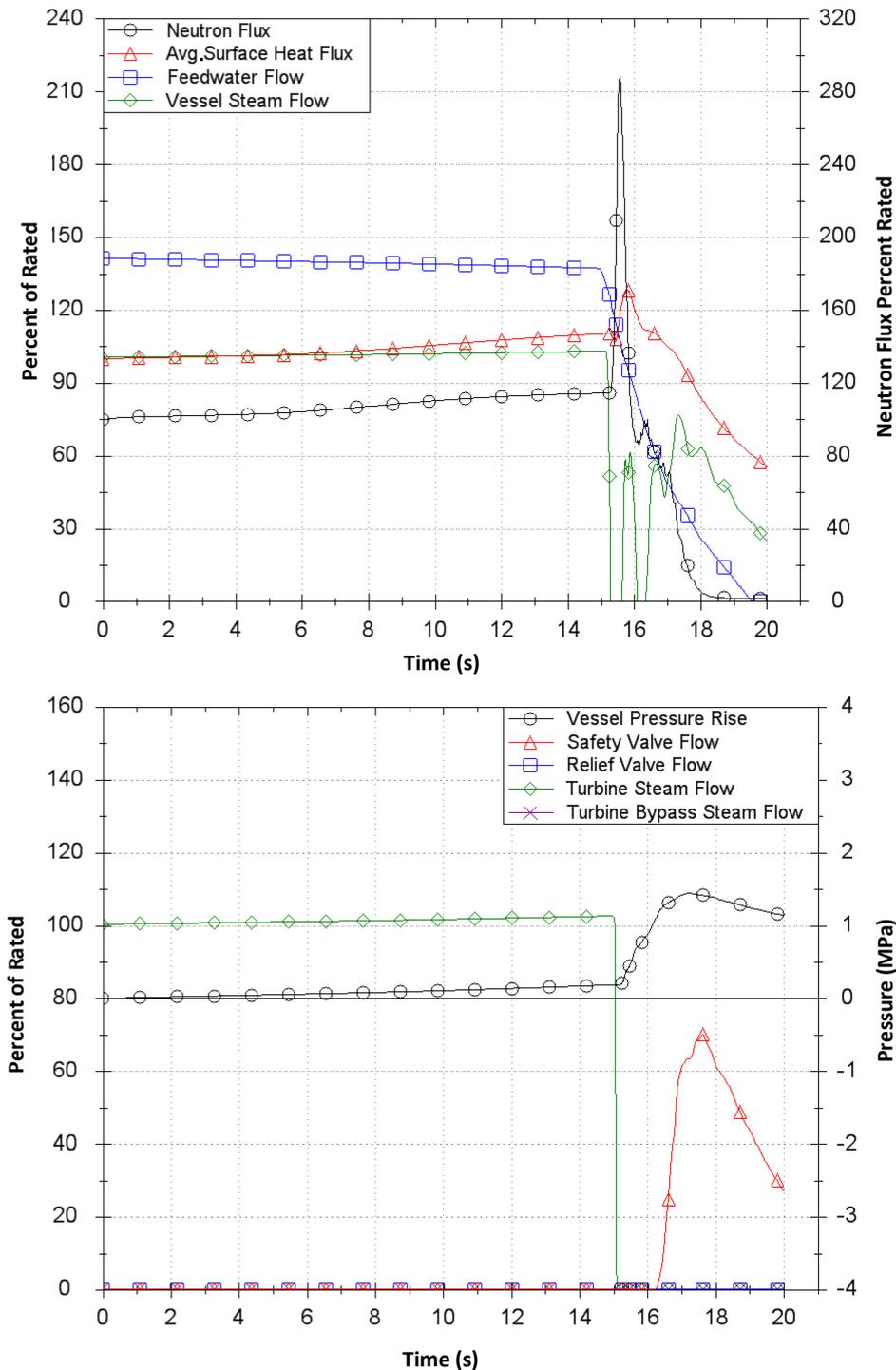


Figure 24.6.4-1: Feedwater Controller Failure – Maximum Demand

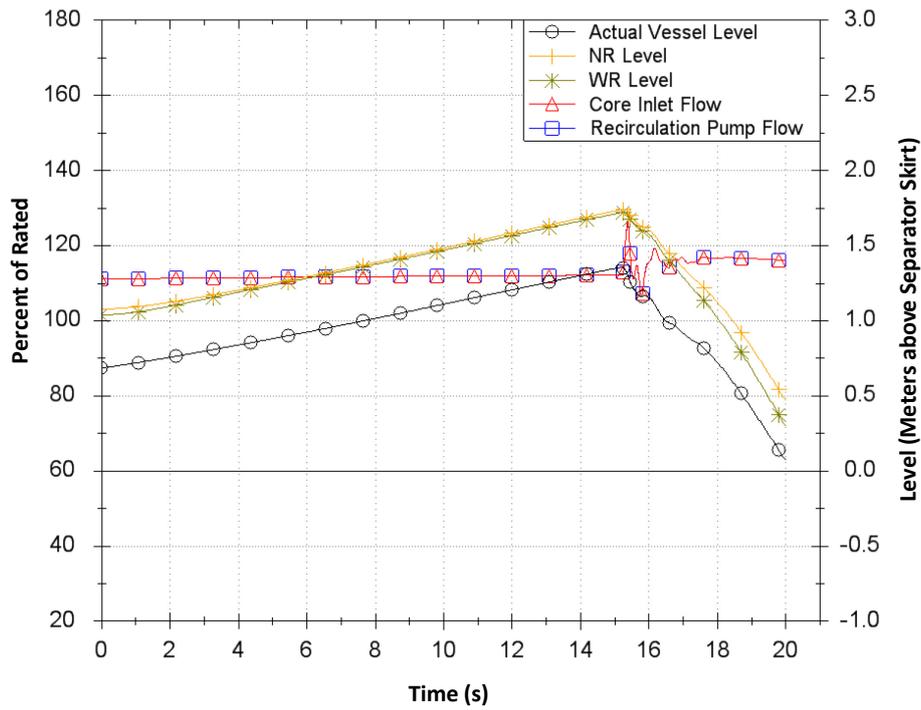


Figure 24.6.4-1: Feedwater Controller Failure – Maximum Demand (Continued)

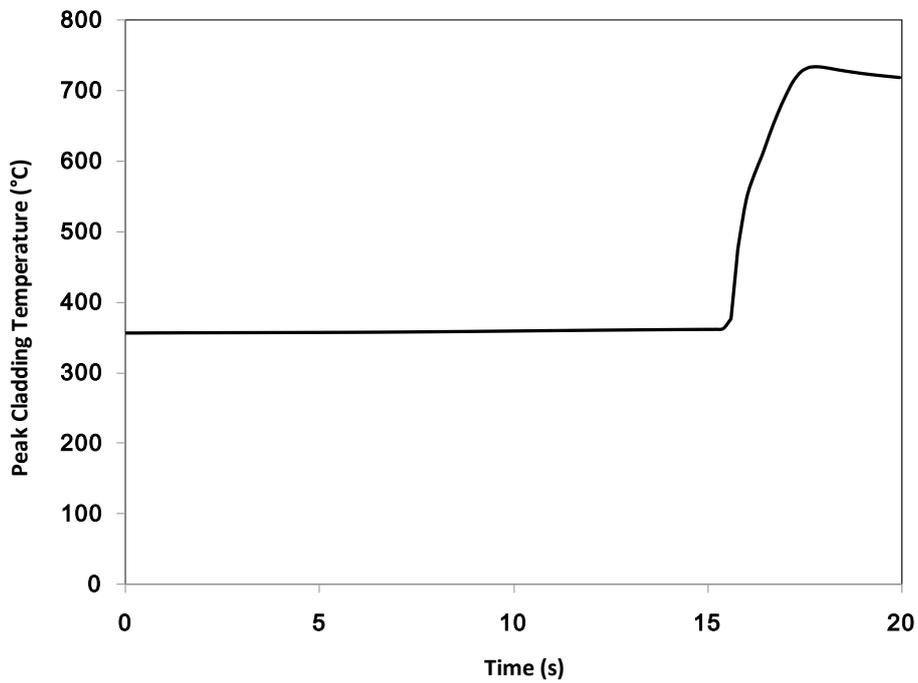
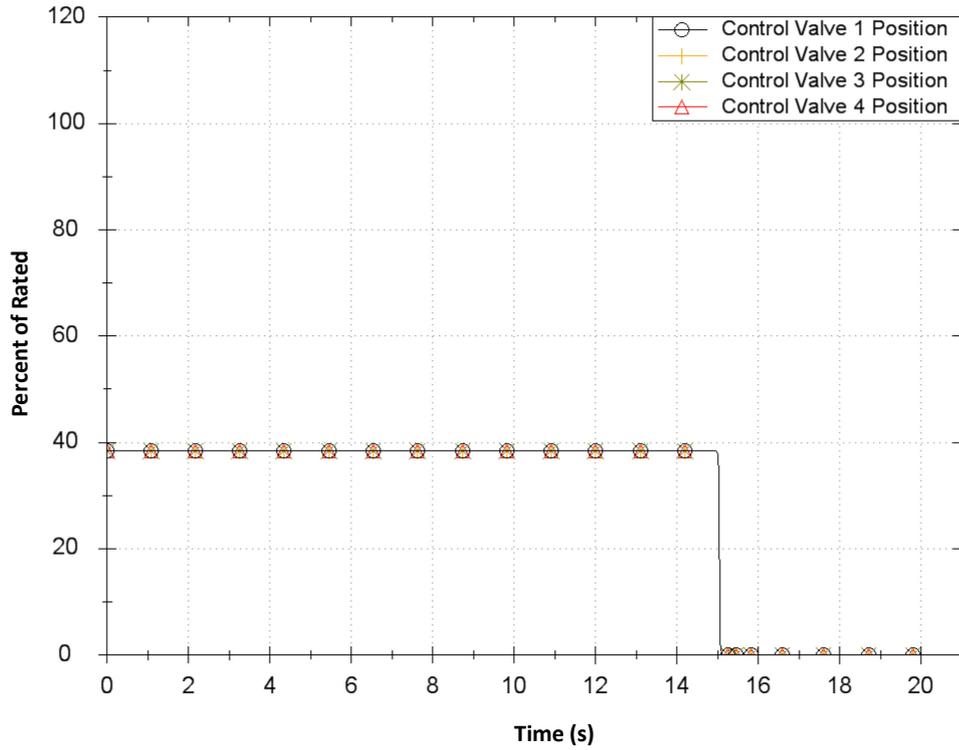


Figure 24.6.4-1: Feedwater Controller Failure – Maximum Demand (Continued)

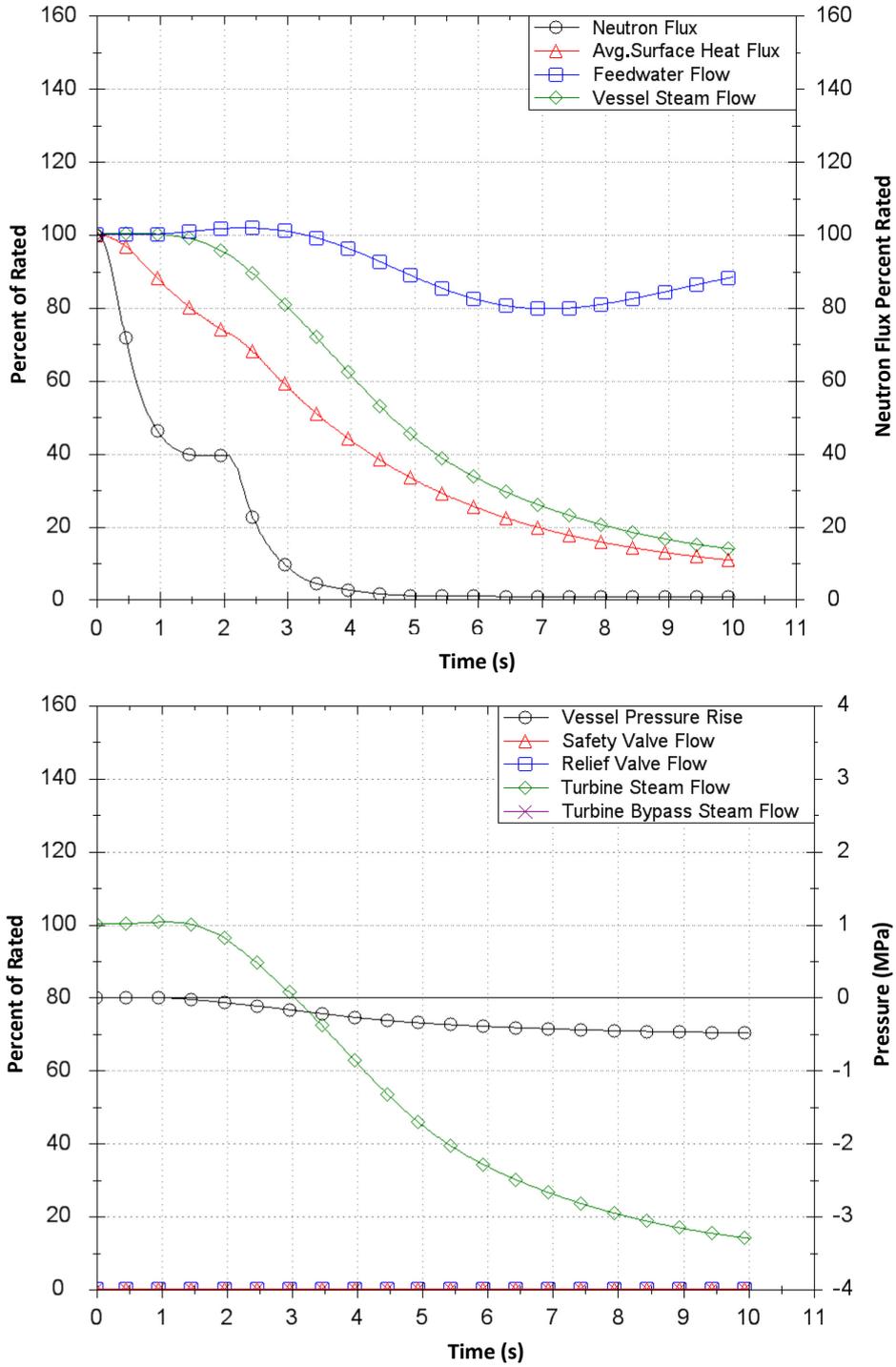


Figure 24.6.4-2: Loss of Reactor Coolant Flow (Trip of All RIPs)

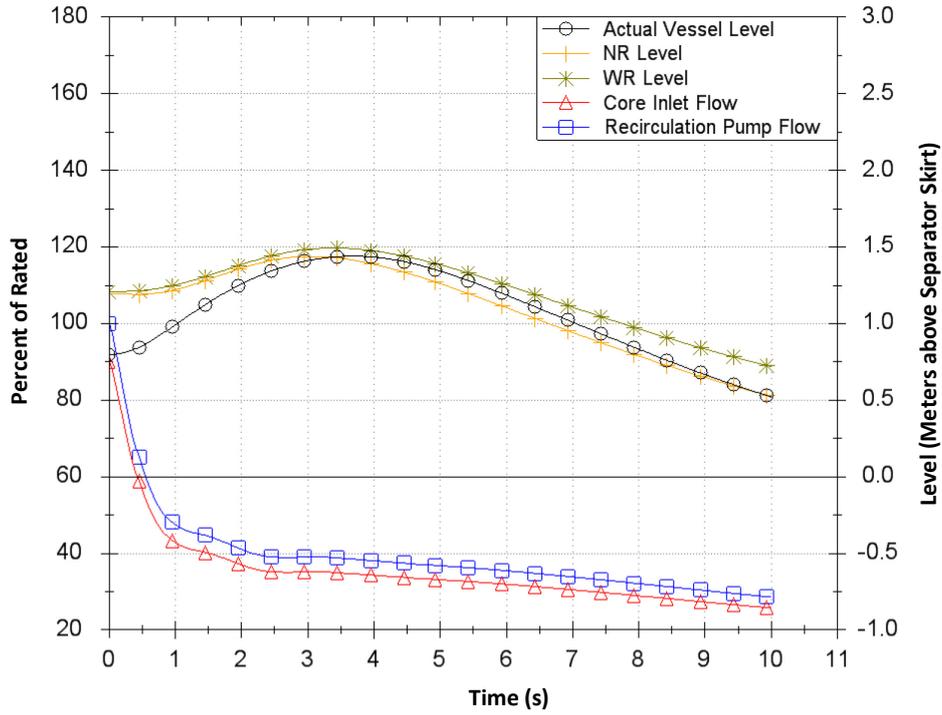


Figure 24.6.4-2: Loss of Reactor Coolant Flow (Trip of All RIPs) (Continued)

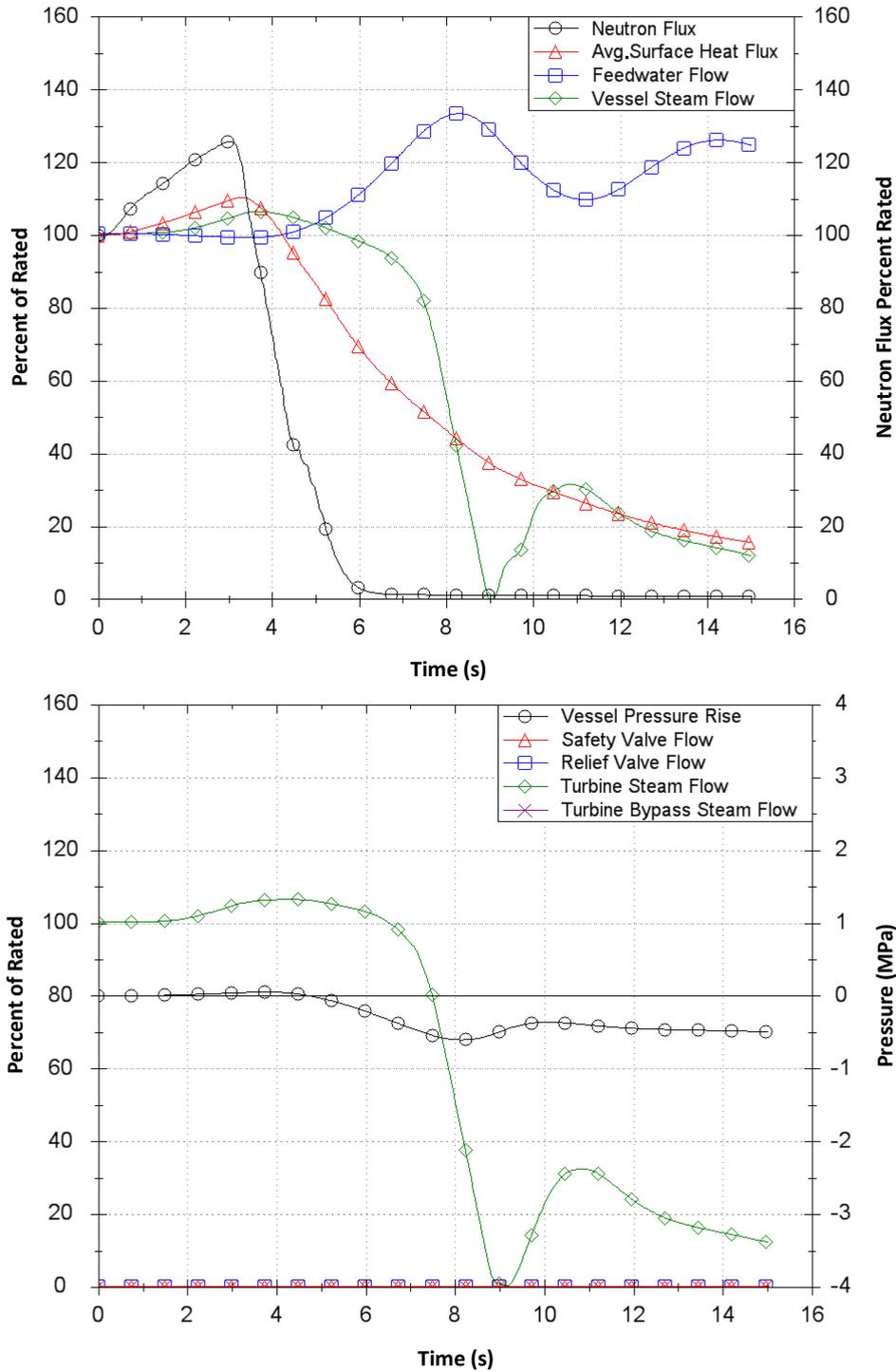


Figure 24.6.4-3: Recirculation Flow Control Failure

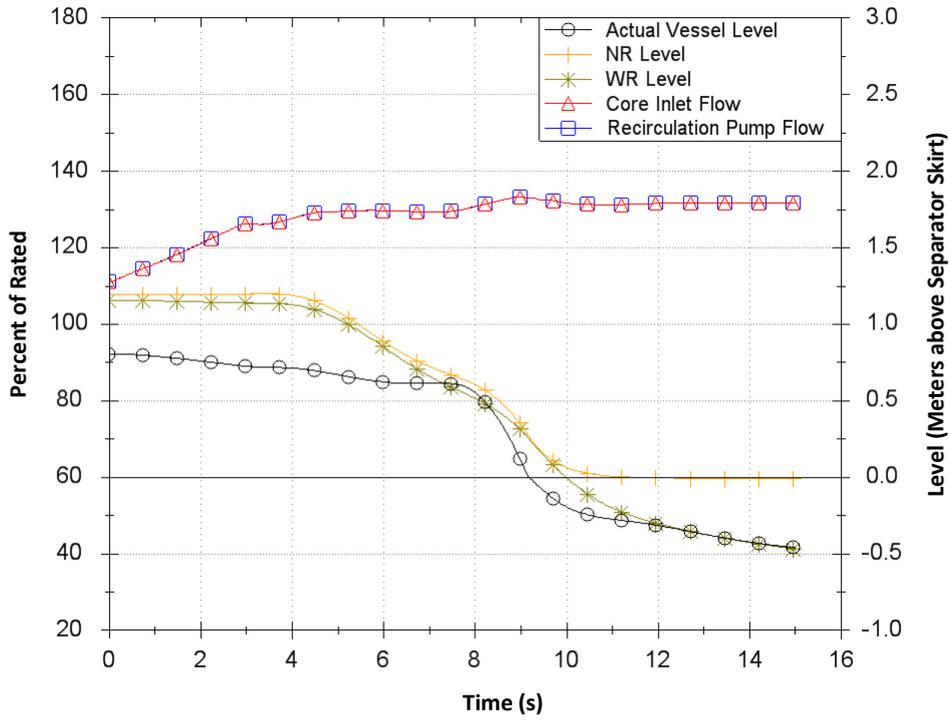


Figure 24.6.4-3: Recirculation Flow Control Failure (Continued)

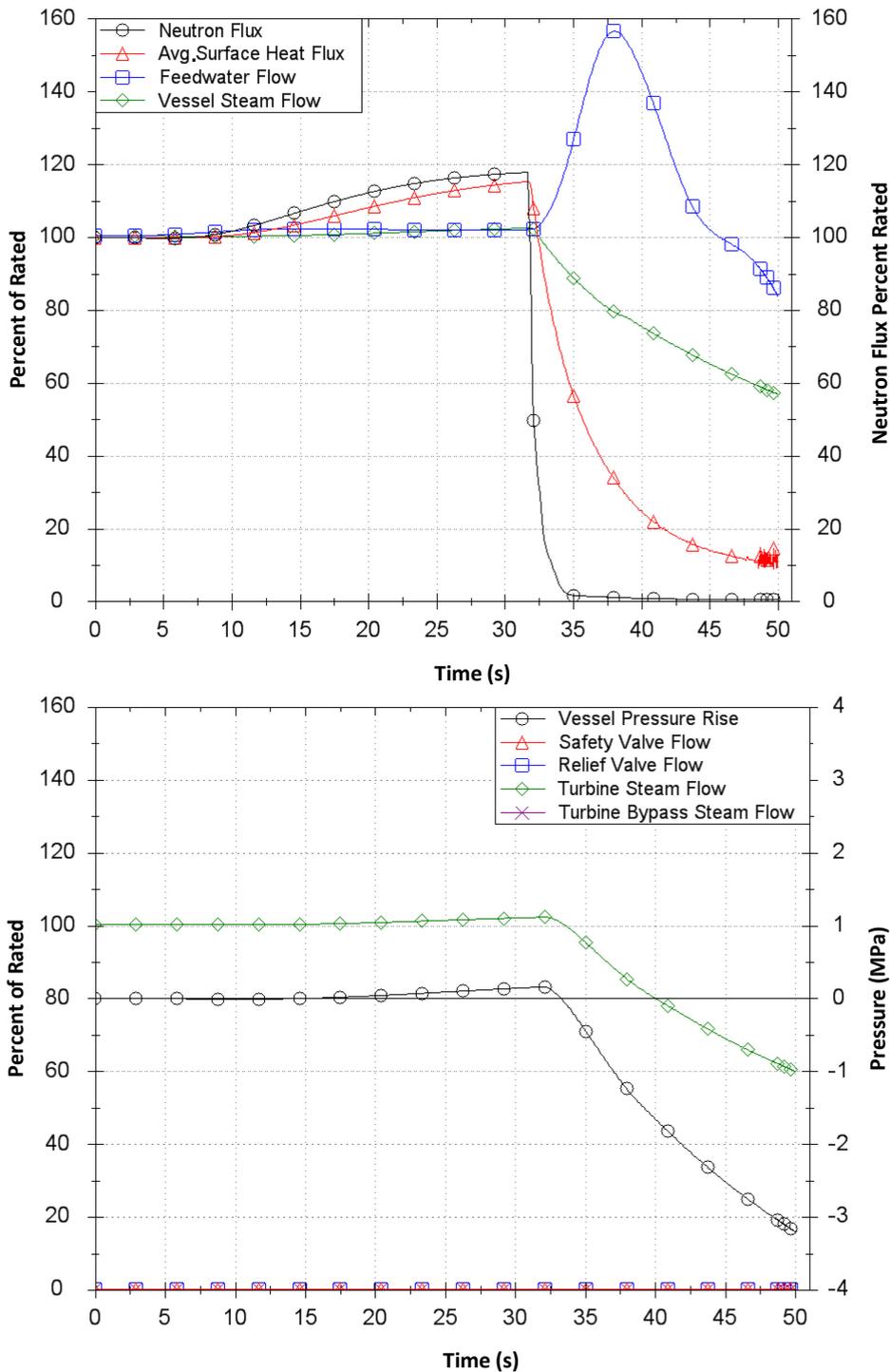


Figure 24.6.4-4: Loss of Feedwater Heating

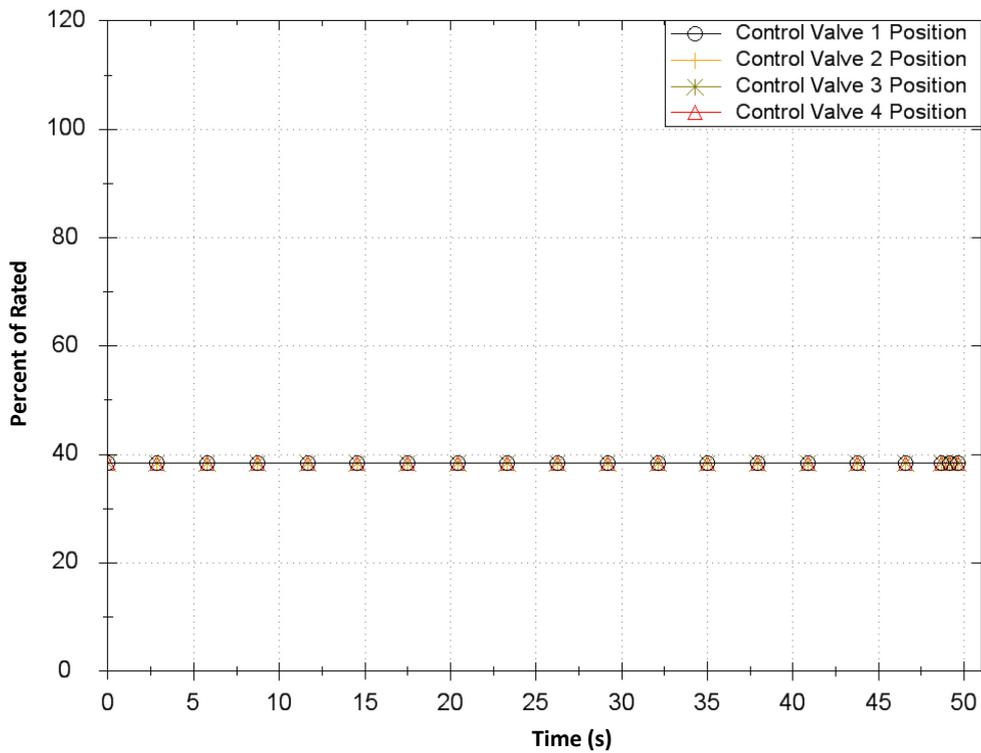
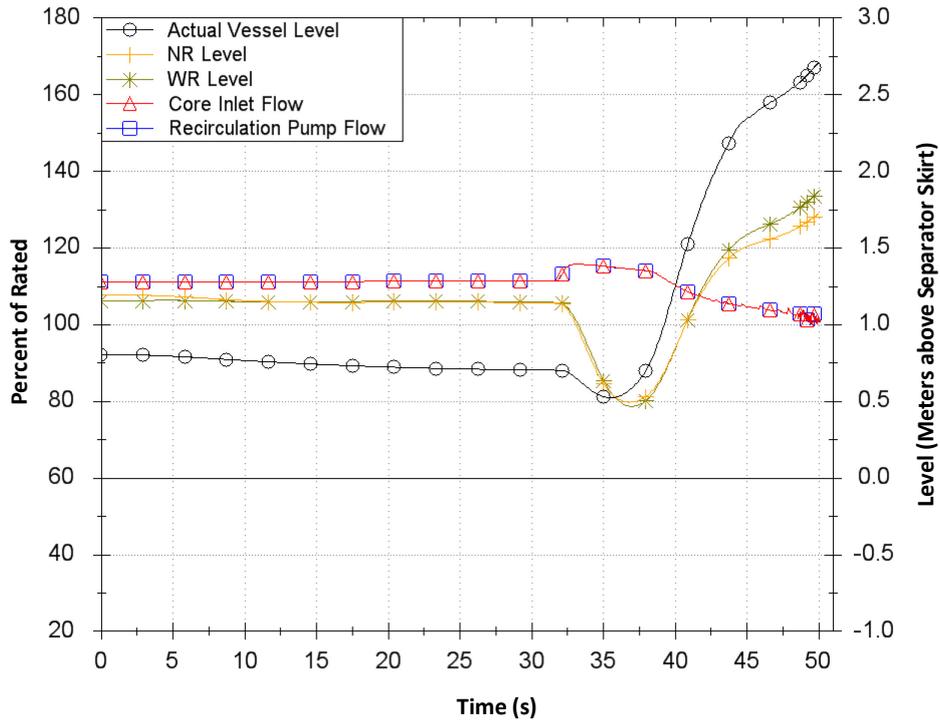


Figure 24.6.4-4: Loss of Feedwater Heating (Continued)

24.6.5 Reactivity and Power Distribution Anomalies

Reactivity and power distribution anomalies are caused by incorrect operation by an operator or malfunction of the Control Rod (CR) system and include the following faults:

- Control Rod Withdrawal Error at Reactor Start-up – see Section 24.6.5.1
- Control Rod Withdrawal Error at Power – see Section 24.6.5.2
- Control Rod Drop – see Section 24.6.5.3

Control Rod Withdrawal Error at Reactor Start-up and Control Rod Withdrawal Error at Power are categorised as frequent design basis fault and Control Rod Drop is categorised as an infrequent design basis fault for UK ABWR.

The SSCs providing protection against these faults are the same as for other non-isolation events and are shown in Table 24.6-1. Initial conditions for the fault are the same as for other non-isolation events and are shown in Table 24.6-2.

24.6.5.1 Control Rod Withdrawal Error at Reactor Start-up

Fault Schedule Ref: 4.1

(1) Description of Fault

At reactor start-up, the control rods are assumed to be continuously withdrawn due to incorrect operation by an operator or a malfunction of Rod Control and Information System (RCIS), resulting in an increase in nuclear reactor power. This fault does not bound any other identified fault. As it is caused by human error or malfunction of class 3 system, it is assumed to be a frequent fault.

The fault has the following features:

- (i) The maximum reactivity worth of a CR group to be withdrawn is limited by the withdrawal procedures. The withdrawal procedures are monitored by the CR Worth Minimiser (RWM).
- (ii) When withdrawing a CR near criticality, the CR shall be withdrawn with monitoring of the reactor period at each step.
- (iii) Abnormal power rise is suppressed by the Doppler Effect.
- (iv) The short reactor period signal from the SRNM blocks CR withdrawal, preventing an abnormal power rise.

- (v) Scram is initiated by the short reactor period signal of SRNM in its intermediate range or the neutron flux high signal of the APRM. The 2 out of 4 logic is applied for Class 1 safety systems. Therefore the system maintains the safety functions even when considering both single failure and maintenance.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the following protections against the fault:

- (i) Control Rod block by SRNM short period or APRM neutron flux signal high (Class 3)
- (ii) Reactor scram initiated by SRNM short period or APRM neutron flux signal high (Class 1)

(3) Analysis of Event

(a) Analysis Assumptions

The following conditions are used in the analysis:

- (i) The nuclear reactor is assumed to be at or near the critical state prior to CR withdrawal. The fuel cladding surface temperature is initially the same as the coolant temperature. The temperatures for different analysis cases are from 20, 100, 160 and 286 °C.
- (ii) The CR withdrawn by error have a worth of 0.030 Δk or more.
- (iii) A CR scram is initiated with a short reactor period of 10 seconds.
- (iv) It is not necessary to assume any water level and pressure change in this event because there is little impact on moderator condition and reactivity in the core.
- (v) It is assumed that one division of each SSC listed in Table 24.6-1 is available.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F6: Fuel enthalpy shall not exceed the design limit in the case of a reactivity insertion fault.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

- (i) The CRs are continuously withdrawn due to incorrect operation or malfunction of the

RCIS.

- (ii) Reactor power increases.
- (iii) Reactor scrams on short reactor period of 10 seconds

(d) Analysis Results

The enthalpy rise for the cases producing the highest blade worth at each temperature are evaluated and the results of the limiting cases which produce the overall highest reactivity increase worth are shown in Table 24.6-9.

A CR scram is initiated before the onset of prompt critical reactivity insertion. The reactor power and enthalpy rise are too small to lead to failure of fuel cladding, so AC-F6 is met. Also the pressure on the reactor coolant pressure boundary is maintained below the maximum allowable working pressure, so AC-R1 is met with some margin.

(4) Discussion and Conclusions

There is no prompt critical reactivity insertion, and as the enthalpy rise is less than the design limit value, there is no failure of fuel cladding. The pressure on the reactor coolant pressure boundary is maintained below the maximum allowable pressure because power is reduced early. Also the pressure on the primary containment boundary is not threatened (AC-C1 met with significant margin). The acceptance criteria described above are met with significant margin.

This fault is fairly benign and makes no claim on any other HLSF except reactor trip, for which there are a number of diverse means. Additional protection is available from Class 1 and Class 2 heat removal functions meaning there is no further reasonably practicable means of reducing the very low risk from this fault. The risk is deemed to be ALARP.

Table 24.6-9: Results Summary for Rod Withdrawal Error at Start-up

Case	Power (MW)	Reactivity (\$)	Enthalpy Rise (kJ/kg)
Initial Core	20	0.37	0.41
Equilibrium Core	16	0.54	0.20

24.6.5.2 Control Rod Withdrawal Error at Power

Fault Schedule Ref: 4.2

(1) Description of Fault

During nuclear reactor power operation, the CRs are assumed to be continuously withdrawn due to incorrect operation by the operator or a malfunction of RCIS, resulting in an increase in nuclear reactor power. The fault does not bound any other faults and, as it is caused by human error or malfunction of Class 3 system, it is assumed to be a frequent fault.

The fault has the following features:

- (i) The Control Rod Block Monitor (RBM) stops control rod withdrawal to prevent an abnormal rise in power when the local power near the withdrawn CR reaches a prescribed level.
- (ii) An alarm on high neutron flux is initiated by the Local Power Range Monitor (LPRM) near the withdrawn control rod to alert the operator.
- (iii) When withdrawing a control rod during power operation, the operating procedures ensure that withdrawal operation is performed whilst checking the local thermal parameters at every step of withdrawal.
- (iv) Scram is initiated by the APRM simulated thermal power high signal. The 2 out of 4 logic is applied for Class 1 safety systems. Therefore the system maintains the safety functions even when considering both single failure and maintenance.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the control rod block by RBM signal high (Class 3), which is same as the analysis shown in the section of “Results with RBM working”.

(3) Analysis of Event**(a) Analysis Assumptions**

The following conditions are used in the analysis:

- (i) To evaluate the change of MCPR and over-power conservatively, the withdrawn CR is assumed to start from a fully inserted state. The initial power is set as the rated power.
- (ii) Analysis is performed for the case of correct operation of the RBM, and for the RBM not working.

- (iii) The RBM generates a CR withdrawal block signal upon reaching 108% of the initial rated power.
- (iv) Reactor scram is initiated by the APRM simulated thermal power high trip of 115%, in the case without the RBM not working.
- (v) It is assumed that one division of each SSC listed in Table 24.6-1 is available.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F1: The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-F3: The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning/creep rupture (perforation) temperature, so as to preclude cladding failure.
- AC-F4: The cladding total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

- (i) The CRs are continuously withdrawn due to incorrect operation or malfunction of the RCIS. Reactor power increases.
- (ii) CR withdrawing is blocked by the RBM, in the case that considers the RBM working
- (iii) Scram is initiated on APRM simulated thermal power high if the RBM does not work.

(d) Analysis Results

- (i) Results with RBM working

At the most limiting point in reactor life, which is at the end of the first sequence exchange of the equilibrium core, gang withdrawal is more severe than single rod withdrawal. Withdrawal of the CR is blocked by the RBM at 29 % withdrawal. The change (reduction) in critical power ratio (Δ CPR) is 0.15, so AC-F1 is met. The transient results in a heat flux increase of approximately 19 % (AC-F2 met) and total core thermal power increase of approximately 11 % but the feedwater flow increases to compensate and nuclear system pressure does not

24. Design Basis Analysis
24.6 Analysis Results and Fault-based View – Non-Isolation Events
Ver. 0

change significantly (AC-R1 met with some margin). With RBM working, this is a fairly benign fault with large margins before any acceptance criterion is challenged.

The nuclear reactor then enters a steady state. However it can return to normal operation by correct CR insertion.

(ii) Results without RBM

If the rod blocking by the RBM does not work, CRs are withdrawn until scram initiation occurs on high neutron flux trip, or APRM simulated thermal power high trip. In this case, the transient results in a heat flux increase of approximately 15%, so AC-F2 is met. The change (reduction) in critical power ratio (Δ CPR) is greater than 0.22. Therefore, it is possible to go below the Safety Limit Minimum Critical Power Ratio (SLMCPR) depending on the initial MCPR value prior to the initiating event.

The evaluation of cladding oxidation, centreline temperature and creep rapture were performed for the cases that go below the SLMCPR, and it is confirmed that the results met the criterion (AC-F3 and AC-F4 met). The details of the evaluation are described in Appendix B.2 of [Ref-5].

(4) Discussion and Conclusions

The MCPR value is greater than the SLMCPR because the change in MCPR is small with correct operation of the RBM. Although the MCPR is below the SLMCPR in the case without RBM, the cladding oxidation, centreline temperature and creep rapture meet the criterion. The surface heat flux of the fuel cladding does not exceed the TOP or MOP acceptance criteria. Pressure on the reactor coolant pressure boundary is maintained below the limit value. Also the pressure on the primary containment boundary is not threatened (AC-C1 met with significant margin). Therefore the acceptance criteria for this event are met.

Operating procedures ensure that withdrawal operation is performed whilst checking the local thermal parameters at every step of withdrawal. This, together with the operation of RBM to block control rod withdrawal when the local power near the withdrawn CR reaches a prescribed level provides additional protection to prevent an abnormal rise in power. No further reasonably practicable means of preventing control rod withdrawal errors have been identified and, given the margins to fuel failure without these protective measures, the risks from this fault are deemed to be ALARP.

24.6.5.3 Control Rod Drop

Fault Schedule Ref: 4.3

(1) Description of Fault

When the reactor is at a critical state or near a critical state, a CR separates from the FMCRD and is assumed to drop from the core, resulting in a fast reactivity input and a change in the power distribution.

This fault bounds the following faults identified in Table 24.4-1:

- Inadvertent reactor scram (CRD pump trip) (Fault Schedule Ref: 4.4)
- Start-up Range Neutron Monitor (SRNM) or Average Power Range Monitor (APRM) sensor failure (Fault Schedule Ref: 4.5)
- Radiation Monitor failure (Fault Schedule Ref: 4.6)

The fault involves the failure of a Class 1 system and is therefore assumed to be an infrequent fault.

The fault has the following features:

- (i) The CR and hollow piston are designed so that they are not separated from each other unless the connection between them is rotated (bayonet coupling).
- (ii) The CR and hollow piston are designed so that they are seated on the ball nut of the CRD by their own weight.
- (iii) If the CR and hollow piston become separated from the ball nut of the CRD, the separation detection mechanism can detect it and block CR withdrawal.
- (iv) If the CR drops, the latch mechanism limits the drop length to 210 mm.
- (v) It is confirmed that the CR and hollow piston are not separated by checking if the CR can be withdrawn further from the full-out position.
- (vi) The CR withdrawal sequence is determined by an operating procedure.
- (vii) The hollow piston is designed so that, even if the CR drops, its dash pot effect limits the CR drop velocity to 0.7 m/s or less.
- (viii) The RWM monitors the CR withdrawal sequence and blocks abnormal withdrawal.
- (ix) Abnormal power rise is suppressed by the Doppler Effect.
- (x) Scram is initiated by the neutron flux high signal.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the reactor scram initiated by SRNM short period or APRM neutron flux signal high (Class 1), which is same as the analysis shown in this section.

(3) Analysis of Event**(a) Analysis Assumptions**

The following conditions are used in the analysis:

- (i) The nuclear reactor is assumed to be at or near the critical state prior to CR drop. The fuel cladding surface temperature is initially the same as the coolant temperature. Analysis is conducted for a range of temperatures from 20, 100, 160 and 286 °C.
- (ii) The drop velocity of the CR is assumed to be 0.7 m/s, as it is limited by the dash pot effect of the hollow piston.
- (iii) A CR scram is initiated by a high neutron flux trip at 120% of rated reactor power.
- (iv) It is not necessary to assume any reactor water level and pressure change in this event because there is little impact on moderator condition and reactivity in the core.
- (v) It is assumed that one division of each SSC listed in Table 24.6-1 is available.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

AC-F7: Fuel enthalpy shall not exceed the limit value to prevent the generation of mechanical energy in the case of reactivity insertion faults.

AC-R2: Pressure on the reactor coolant pressure boundary shall be maintained below 120% of the maximum allowable working pressure.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

- (i) When the reactor is in a critical state or near a critical state, a CR separates from the FMCRD and drops to the FMCRD position.
- (ii) Reactor power increases.
- (iii) The power increase is suppressed by the Doppler Effect.

- (iv) A CR scram is initiated by a high neutron flux trip at 120% of rated reactor power.

(d) Analysis Results

The results of the CR worths calculated for various combinations of exposure and moderator temperatures are less than 0.017 Δk. The results of the limiting cases in terms of the over power and enthalpy are shown in Table 24.6-10. Reactivity insertion is suppressed by the Doppler Effect during this event. The reactor power and enthalpy rise are too small to lead to failure of the fuel cladding. Also the pressure on the reactor coolant pressure boundary is maintained below the maximum allowable working pressure (AC-R2 met with significant margin).

(4) Discussion and Conclusions

As the enthalpy rise is less than the design limit (AC-F7 met), there is no failure of the fuel cladding. The pressure on the reactor coolant pressure boundary is maintained below the maximum allowable pressure because power is reduced early. Also the pressure on the primary containment boundary is not threatened (AC-C1 met with significant margin). Therefore the acceptance criteria described above are met.

This fault is fairly benign and makes no claim on any other HLSF except reactor trip, for which there are a number of diverse means. Additional protection is available from Class 1 and Class 2 heat removal functions meaning there is no further reasonably practicable means of reducing the very low risk from this fault. The risk is deemed to be ALARP.

Table 24.6-10: Results Summary for Control Rod Drop

Case	Power (MW)	Enthalpy Rise (kJ/kg)
Initial Core	2772	1.76×10^2
Equilibrium Core	12492	3.03×10^2

24.7 Analysis Results and Fault-based View – Isolation Events

Isolation events are faults that shut off the main steam going to turbine due to the closure of main steam isolation valves or due to the closure of main stop valves or turbine control valves without opening turbine bypass valves. Isolation events fall into three categories:

- Increase in reactor pressure – see Section 24.7.1
- Decrease in reactor coolant inventory (decrease in RPV water level) – see Section 24.7.2
- Loss of off-site power – see Section 24.7.3

In this section, the analysis of the representative isolation events is presented. The analyses of the other isolation events are described in A.5.2 in Topic Report on DBA [Ref-5] and these events results comply with all acceptance criteria.

Table 24.7-1 shows the HLSFs claimed in the analysis of isolation events and the Class 1 systems that provide them.

Table 24.7-1: Provision of HLSFs by Class 1 systems for Isolation Events

HLSF	System	PCSR Ref	Notes
1-3 Emergency shutdown of the reactor	CRD	11.5.2, 12.4.3.1	The corresponding setpoints are shown in Table 24.6-3 and performance is shown in Table 24.6-4.
2-1 Functions to cool reactor core	RCIC	13.4	Power for HPCF is provided by EDGs
	HPCF	13.4	
	SRV	12.3.5.2	
3-1 Functions to remove residual heat after shutdown	SRV	12.3.5.2	SRV depressurises reactor so that RHR can function. Power for RHR provided by EDG. Heat is rejected to RCW and RSW
	RHR	12.3.5.4	
	SSLC	14.6.2.1	SSLC provides the functions to control SSCs related to SRV and RHR.
4-2 Functions to prevent overpressure within the reactor coolant pressure boundary	SRV	12.3.5.2	Safety valve function of SRVs

**Table 24.7-1: Provision of HLSFs by Class 1 systems for Isolation Events
(Continued)**

HLSF	System	PCSR Ref	Notes
4-7 Functions to confine radioactive materials, shield radiation, and reduce radioactive release	MSIV	12.3.5.2	MSIV is closed to isolate the reactor.
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SSLC	14.6.2.1	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system.
5-2 Supporting functions especially important to safety	Class 1 EPS	15.3	Class 1 EPS supplies power to the first line of safety systems. EDG supports SSCs related to HPCF and RHR.
	RCW/RSW	16.3.2	RCW/RSW are essential systems for supporting HPCF, RHR and Class 1 HVAC operations.
	UHS	16.3.1	UHS provides sufficient cooling water to the RSW.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 1 HVAC	16.5	Class 1 HVAC ensures the adequate environmental parameters for Class 1 SSCs are maintained.
	HECW	16.3.5.1	HECW provides chilled water for Class 1 HVAC.

Major Plant Specifications related to Setpoints of Safety Systems and other to other items are shown in Table 24.6-3 and Table 24.6-4.

In this section, the analyses presented, assume only the above Class 1 safety systems are available and actuate, that is, correct performance of lower class systems such as the recirculation pump trip and the turbine bypass valves are not assumed where this would alleviate the consequences.

Many of the events considered in this section are frequent faults and require diverse provision of the above HLSFs. The demonstration that the faults can be protected by Class 2 SSCs is given in Section 24.12.

The initial conditions for the analyses are shown in Table 24.6-2.

Limits and Conditions for Operation

The following LCO is identified in addition to those in Section 24.6:

The future licensee shall ensure that, during normal power operation, one or more divisions of the following systems are operational even if one division is unavailable due to testing or maintenance and another division is unavailable due to a single failure:

- EDG

The future licensee shall ensure that, during normal power operation, the following SSCs are operational:

- MSIV

24.7.1 Increase in Reactor Pressure

24.7.1.1 Load Rejection with Failure of All Bypass Valves

Fault Schedule Ref: 1.1

(1) Description of Fault

Fast closure of the turbine control valves (TCVs) is initiated whenever electrical grid disturbances occur which result in significant loss of electrical load on the generator. The TCVs are required to close as rapidly as possible to prevent excessive overspeed of the turbine-generator rotor. Closure of the main TCVs, with no opening of the Turbine Bypass Valves (TBVs), causes a sudden reduction in steam flow, which results in an increase in system pressure and reactor shutdown.

This fault bounds of the following faults:

- Generator load rejection with failure of all bypass valves (Fault Schedule Ref: 1.1)
- Inadvertent MSIV closure (Fault Schedule Ref: 2.1)
- Reactor pressure regulator failure in the open direction (Fault Schedule Ref: 2.2)
- Loss of main condenser vacuum (Fault Schedule Ref: 2.3)

Among these events, the limiting event for PCT, core average surface heat flux, and vessel bottom pressure is Load rejection with failure of all bypass valves. Therefore, the analysis of Load rejection with failure of all bypass valves is presented below. This fault is assumed to be a frequent fault.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the following protections against the fault:

- (i) Reactor scram (Class 1) and trip of 4 RIPs (Class 3) initiated by rapid TCV closure
- (ii) Opening of the turbine bypass valves (Class 3)
- (iii) Opening of the SRV (Relief valve function) (Class 3)

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (ix) below. Further details of the analysis conditions are described in A.5.2.1.3 in Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2.
- (ii) The closure characteristics of the TCVs are assumed such that the valves operate in the full arc (FA) mode and have a full stroke closure time, from fully open to fully closed, of 0.15 seconds. (In the analysis, less than 0.15 seconds is required to close the valve because the valve is not fully open at the beginning of the transient.)
- (iii) The TBVs are assumed to not operate, as defined by the fault.
- (iv) The RIP trip function is not assumed to operate (but a sensitivity with correct operation is performed)
- (v) The initial core flow is assumed to be 111%, which gave the most severe results in sensitivity analysis.
- (vi) The operating mode of the RFC (Class 3) is assumed to be manual (frozen).
- (vii) The EHC (Class 3) does not affect the event since the TCV closes and the TBV is not assumed to operate.
- (viii) The FDWC (Class 3) is assumed to be working.
- (ix) One division of each of the SSCs listed in Table 24.7-1 is assumed to be available.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F3: The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning/creep rupture (perforation) temperature, so as to preclude cladding failure.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

The reactor power rapidly increases due to the vessel pressure increase caused by the generator load rejection with TCV rapid closure. However, the TCV rapid closure initiates the reactor scram and the maximum neutron flux and the surface heat flux are limited to 269% and 118% of normal values, respectively. Increased reactor pressure is alleviated by the SRV (safety function) to a maximum of 8.46 MPa [gauge]. The Δ CPR for this event is 0.25. Therefore, in case of an OLMCPR value of 1.28,

24. Design Basis Analysis
24.7 Analysis Results and Fault-based View – Isolation Events
Ver. 0

the MCPR falls below the safety limit MCPR (1.06) after the initiating event. With the boiling transition, the coefficient of heat transfer from the fuel cladding to the coolant becomes small, and the fuel cladding temperature increases. However, the temperature increase stops after a short time because the reactor is scrammed. The peak cladding temperature during this fault is about 624 °C.

(d) Analysis Results

The results of the analysis of the Load rejection with failure of all bypass valves are shown in Table 24.7-2 and Figure 24.7.1-1.

In the analysis, the MCPR is below the safety limit MCPR but the peak cladding temperature is below the limiting value of 800 °C. The results are compared with the acceptance criteria described above as follows:

- The calculated maximum fuel cladding temperature is about 624 °C, and so does not exceed 800 °C. In addition, ballooning rupture does not occur in any of the fuel rods. (AC-F3 met with some margin)
- The peak surface heat flux of the fuel cladding is approx. 118%, and so does not exceed the acceptance criterion 138%. (AC-F2 met with some margin)
- The peak pressure on the reactor coolant pressure boundary is 8.71 MPa [gauge], and so it does not exceed the acceptance criterion 9.48 MPa [gauge]. (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not exceed the maximum allowable working pressure. (AC-C1 met with significant margin)

(4) Discussion and Conclusions

There are a number of Class 3 SSCs that also provide the HLSFs claimed in this analysis. Table 24.7-3 shows the system parameters if these SSCs function correctly. It is noted that if correct performance of lower class RIP trip system and SRV (Relief valve) is assumed, the transient behaviour of this event is milder, and therefore, in the case of an OLMCPR value of 1.28 or more, the MCPR is greater than 1.06 and remains above the safety limit MCPR (1.06) as shown in Table 24.7-2.

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met with some margin.

The defence in depth provided by these lower class systems and the margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

Table 24.7-2: Results Summary for Load Rejection with Failure of All Bypass Valves (Event Leading to Increase in Core Pressure)

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR	PCT (°C)
No RIP trip assumed Figure 24.7.1-1	269	8.71	118	> 0.22	624
Case of correct performance of lower class RIP trip system assumed	199	8.41	108	0.22	N/A

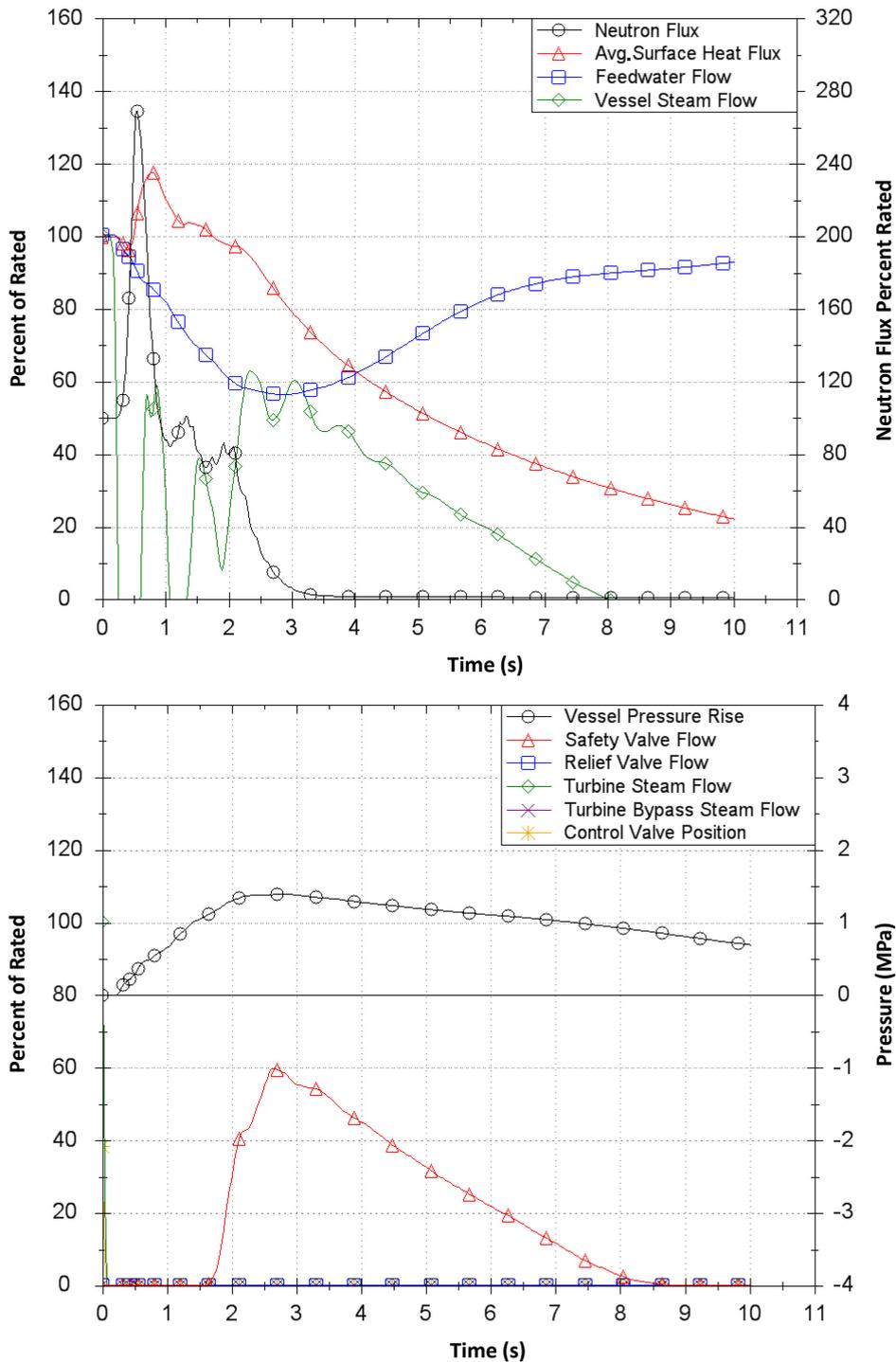


Figure 24.7.1-1: Generator Load Rejection with Failure of All Bypass Valves

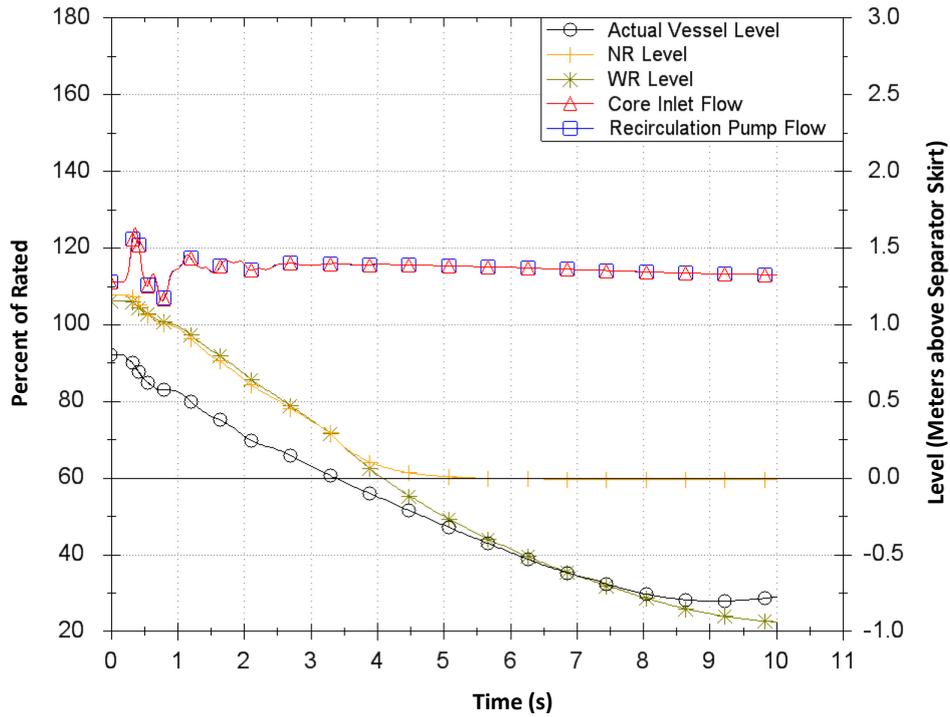


Figure 24.7.1-1: Generator Load Rejection with Failure of All Bypass Valves (Continued)

24.7.2 Decrease in Reactor Coolant Inventory (RPV Water Level Decrease Events)

24.7.2.1 Loss of All Feedwater Flow

Fault Schedule Ref: 3.1

(1) Description of Fault

During power operation of the reactor, failure of the Feedwater Control system (FDWC) or trip of the feedwater pumps results in partial loss of the feedwater flow or loss of all feedwater flow, and the reactor water level drops.

This fault does not bound any other faults and is assumed to be a frequent fault as it involves the failure of a Class 3 system.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the following protections against the fault:

- (i) Reactor scram (Class 1) and trip of 4 RIPs (Class 2) initiated by Level 3 signal
- (ii) RCIC injection (Class 1) and trip of 6 RIPs (Class 2) initiated by Level 2 signal

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions for the analysis are listed in (i) to (x) below. Further details of the analysis conditions are described in A.5.3.1.1 in Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2.
- (ii) Loss of all feedwater flow is analysed as the most severe case.
- (iii) Operation of the standby feedwater pumps is not assumed.
- (iv) Taking the feedwater pump inertia into consideration, approx. 5 seconds is assumed for the feedwater flow to be completely lost.
- (v) The reactor core isolation cooling system is not assumed to operate.
- (vi) The initial core flow is assumed to be 90% as a representative case, since it has no effect on the comparisons of the results against the acceptance criteria.
- (vii) The operating mode of the RFC (Class 3) is assumed to be manual (frozen).
- (viii) The EHC (Class 3) is assumed to be working.

24. Design Basis Analysis

24.7 Analysis Results and Fault-based View – Isolation Events

Ver. 0

- (ix) The FDWC (Class 3) does not affect the event since the feedwater pumps trip in the case analysed.
- (x) One division of each of the SSCs listed in Table 24.7-1 is available.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent event, they are:

- AC-F1: The critical power ratio (CPR) shall be greater than the safety limit CPR (MCPR) so as to maintain nucleate boiling.
- AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.
- AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.
- AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

The loss of feedwater flow causes the reactor water level to drop rapidly because of the mismatch between the incoming feedwater flow to the vessel and the outgoing steam flow. Therefore, reactor scram occurs initiated by low reactor water level scram (Level 3). The transient is gradual because the reactor is already scrammed by this time, and the power has decreased sufficiently. The neutron flux, the surface heat flux and the vessel pressure do not exceed their initial values. The Δ CPR for this event is not limiting. This transient has the severest water level drop of all the transients analysed in this section. However, even in this case, the High Pressure Core Flooder system starts up at a low reactor water level (Level 1.5) to prevent the reactor water level from dropping.

(d) Analysis Results

The analysis results of the Loss of all feedwater flow are shown in Table 24.7-3 and Figure 24.7.2-1.

The MCPR is greater than the safety limit MCPR. The results are compared with the acceptance criteria described above as follows:

- The Δ CPR is negligible, and so the MCPR remains above the safety limit MCPR (1.06). (AC-F1 met)
- The surface heat flux does not exceed the initial value. (AC-F2 met with significant margin)

- The peak pressure on the reactor coolant pressure boundary is 7.29 MPa [gauge], and so it does not exceed the acceptance criterion 9.48 MPa [gauge]. (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not change (No SRVs work in this event). (AC-C1 met with significant margin)

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met. As a result, there are no radiological releases and no exposure of workers or the public.

Because the MCPR is below the safety limit MCPR, there is significant margin before the fuel acceptance criteria would be threatened. The same applies to the reactor pressure boundary acceptance criterion.

The margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

Table 24.7-3: Results Summary for Loss of All Feedwater Events

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR
Figure 24.7.2-1	100	7.29	100	Note 1

Note 1: Not limiting for Δ CPR

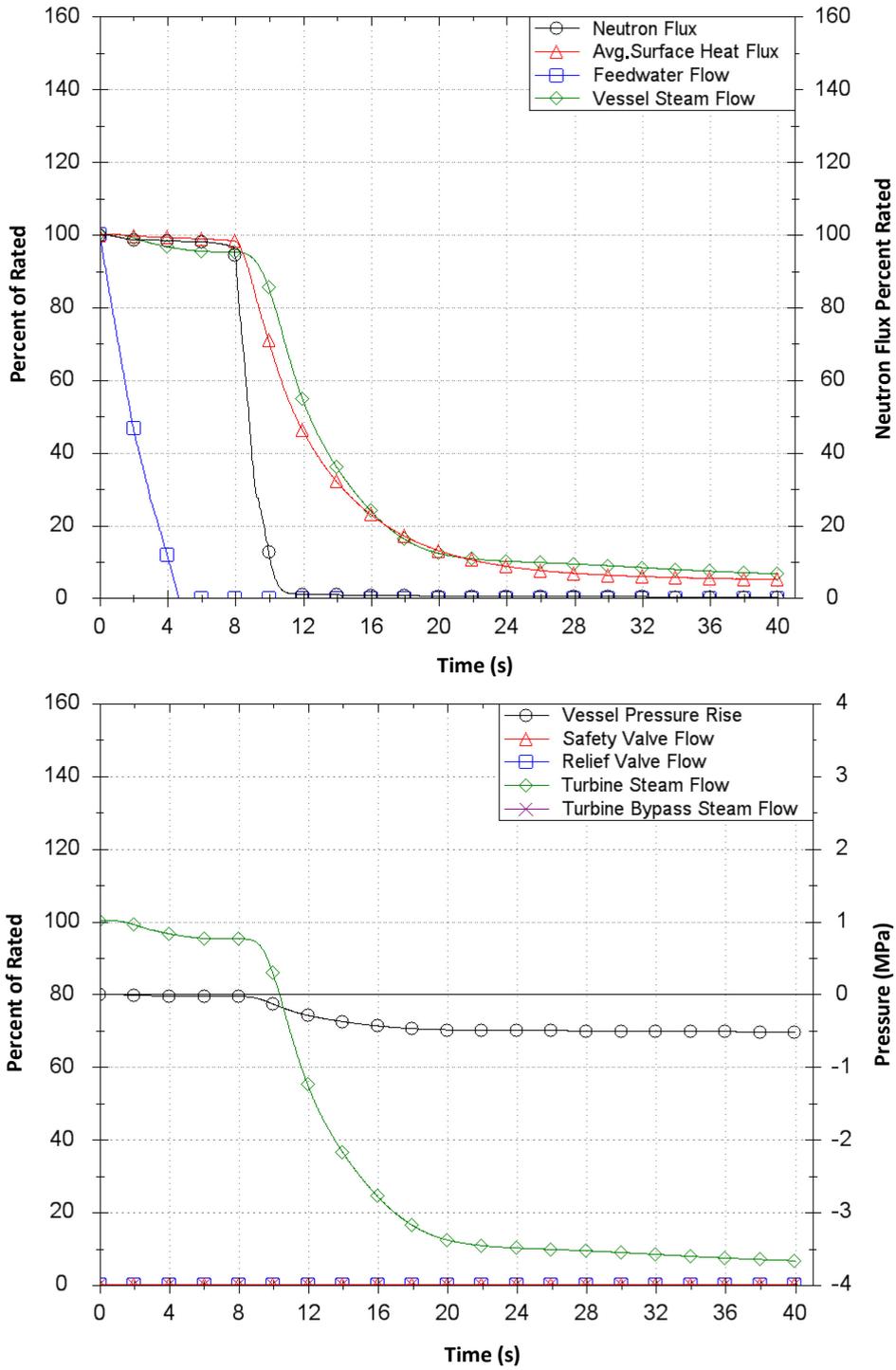


Figure 24.7.2-1: Loss of All Feedwater Flow

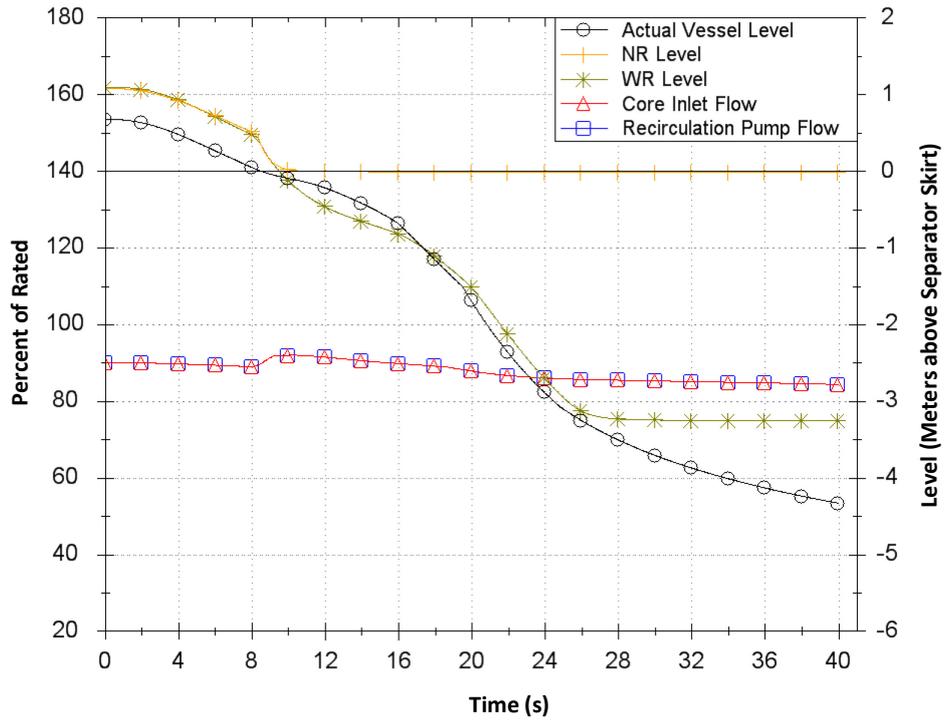


Figure 24.7.2-1: Loss of All Feedwater Flow (Continued)

24.7.3 Loss of Off-site Power

In this section, the analysis of the representative Loss of Off-site Power event is presented.

Loss of off-site power comprises three events in the DB Fault Schedule:

- Short term Loss of Off-site Power (Fault Schedule Ref: 5.1)
- Medium term Loss of Off-site Power (Fault Schedule Ref: 5.2)
- Long term Loss of Off-site Power (Fault Schedule Ref: 5.3)

Among these faults Short term Loss of Off-site Power is representative because the other faults are the same as Short term Loss of Off-site Power in the first 2 hours and are stabilised by the ECCS after that.

Short term and Medium term LOOP are frequent faults although Long term Loop in the group is an infrequent fault.

The protection against the fault is the same as for other isolation events and given in Table 24.7-1.

24.7.3.1 Short Term LOOP

Fault Schedule Ref: 5.1

(1) Description of Fault

During power operation of the reactor, off-site power is lost because of a failure of the external grid or of the on-site power facilities. It is accompanied by generator load rejection on the external grid failure, or turbine trip on the on-site power facilities failure. A generator load rejection is analysed here, since it results ultimately in a loss of normal power supply to the house auxiliaries.

(2) Plant Normal Response

In practice, the occurrence of this event would lead to the following protections against the fault:

- (i) Reactor scram initiated by rapid TCV closure (Class 1)
- (ii) MG set prevent rapid core flow coastdown (Class 3)
- (iii) Opening of the turbine bypass valves (Class 3)

- (iv) Opening of the SRV (Relief valve function) (Class 3)

(3) Analysis of Event**(a) Analysis Assumptions**

The analysis conditions for the analysis are listed in (i) to (xiii) below. Further details of the analysis conditions are described in A.5.4.1.1 in Topic Report on DBA [Ref-5].

- (i) The initial plant conditions of this analysis are shown in Table 24.6-2.
- (ii) Assuming that a generator load rejection occurs because of loss of off-site power, the TCVs close rapidly and the reactor scrams. As a result, supply of all normal power to the house auxiliaries is lost.
- (iii) When the normal on-site power is lost, the house auxiliaries such as RIPs, circulating water pumps and condensate pumps trip, and the following occurs.
- The circulating water pump trip causes a loss of condenser vacuum, which leads to the turbine trip and the MSIV closure
 - Following the circulation pump trip, turbine driven feedwater pumps trip on lowered suction pressure and the vessel water level decreases.
 - However the vessel pressure rises because of the TCV rapid closure, it is suppressed by the SRVs (safety function)

Thus, various phenomena occur in combination. Here, however, the following state is considered:

- (iv) Loss of grid connections occurs at time < 0 .
- (v) The loss of the condensate pumps causes trip of the feedwater pumps due to low suction pressure. This is assumed to occur at 5 seconds.
- (vi) Loss of on-site power causes trip of all RIPs since the Motor-Generator (M-G) sets are not assumed to operate.
- (vii) Loss of on-site power causes loss of condensate pumps and loss of main condenser circulating water pumps at time = 0
- (viii) The TBVs are not assumed to operate.
- (ix) The initial core flow is assumed to be 90%, which gave the most severe result in sensitivity analysis.
- (x) The RFC (Class 3) does not affect the event since all RIPs are lost.
- (xi) The EHC (Class 3) does not affect the event since the TCV closes and the TBV is not assumed to operate.

(xii) The FDWC (Class 3) is assumed to be working.

(xiii) One division of each SSC listed in Table 24.7-1 is available

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, they are:

AC-F3: The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning/creep rupture (perforation) temperature, so as to preclude cladding failure.

AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.

AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

In the very early stage of the event, the void fraction may decrease due to the increasing vessel pressure caused by interruption of the main steam flow. On the other hand, the core flow decreases rapidly since all RIPs are tripped, therefore a large change in void fraction does not occur. In addition, the reactor is scrammed and the neutron flux and the surface heat flux do not exceed their initial value. The SRV (safety function) opens when the pressure reaches the setpoint and the reactor pressure is limited to approximately 8.43 MPa [gauge]. The Δ CPR for this event is 0.24. Therefore, in the case of an OLMCPR value of 1.28, the MCPR falls below the safety limit MCPR (1.06) due to the rapid reduction in the flow rate by loss of RIP power. In this case, the fuel cladding temperature increases because of smaller heat transfer coefficient due to the boiling transition. However, the temperature increase stops after a short time because the reactor is scrammed. The peak cladding temperature during this event is about 575 °C.

(d) Analysis Results

The results of the analysis of loss of off-site power are shown in Table 24.7-4 and Figure 24.7.3-1.

In the analysis, the MCPR is below the safety limit MCPR. The results are compared with the acceptance criteria above as follows:

- The calculated maximum fuel cladding temperature is about 575 °C, and so does not exceed

800 °C. In addition, ballooning rupture does not occur in any of the fuel rods. (AC-F3 met with significant margin)

- The peak surface heat flux of the fuel cladding does not exceed the initial value. (AC-F2 met with significant margin)
- The peak pressure on the reactor coolant pressure boundary is 8.53 MPa [gauge], and so it does not exceed the acceptance criterion 9.48 MPa [gauge]. (AC-R1 met with some margin)
- The pressure on the reactor containment boundary does not exceed the maximum allowable working pressure. (AC-C1 met with significant margin)

(4) Discussion and Conclusions

It is noted that if correct performance of lower class systems, that is the M-G sets and the SRV (Relief valve) and the TBVs, is assumed, the transient behaviour of this event is milder, such that in the case of an OLMCPR value of 1.28 or more, the MCPR is greater than 1.14 and remains above the safety limit MCPR (1.06), as shown in Table 24.7-4.

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met, mainly with significant margin.

There are a number of Class 3 SSCs providing the HLSFs claimed in this analysis in addition to the Class 1 SSCs in Table 24.6-1. Table 24.7-4 shows the system parameters if these SSCs function correctly. The defence in depth provided by these lower class systems and the margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

Table 24.7-4: Results Summary for Loss of Off-site Power

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	ΔCPR	PCT (°C)
No lower class systems operate Figure 24.7.3-1	100	8.53	100	> 0.22	575
Case of correct performance of lower class systems assumed (M-G sets and TBV)	140	8.07	100	0.14	N/A

24. Design Basis Analysis
 24.7 Analysis Results and Fault-based View – Isolation Events
 Ver. 0

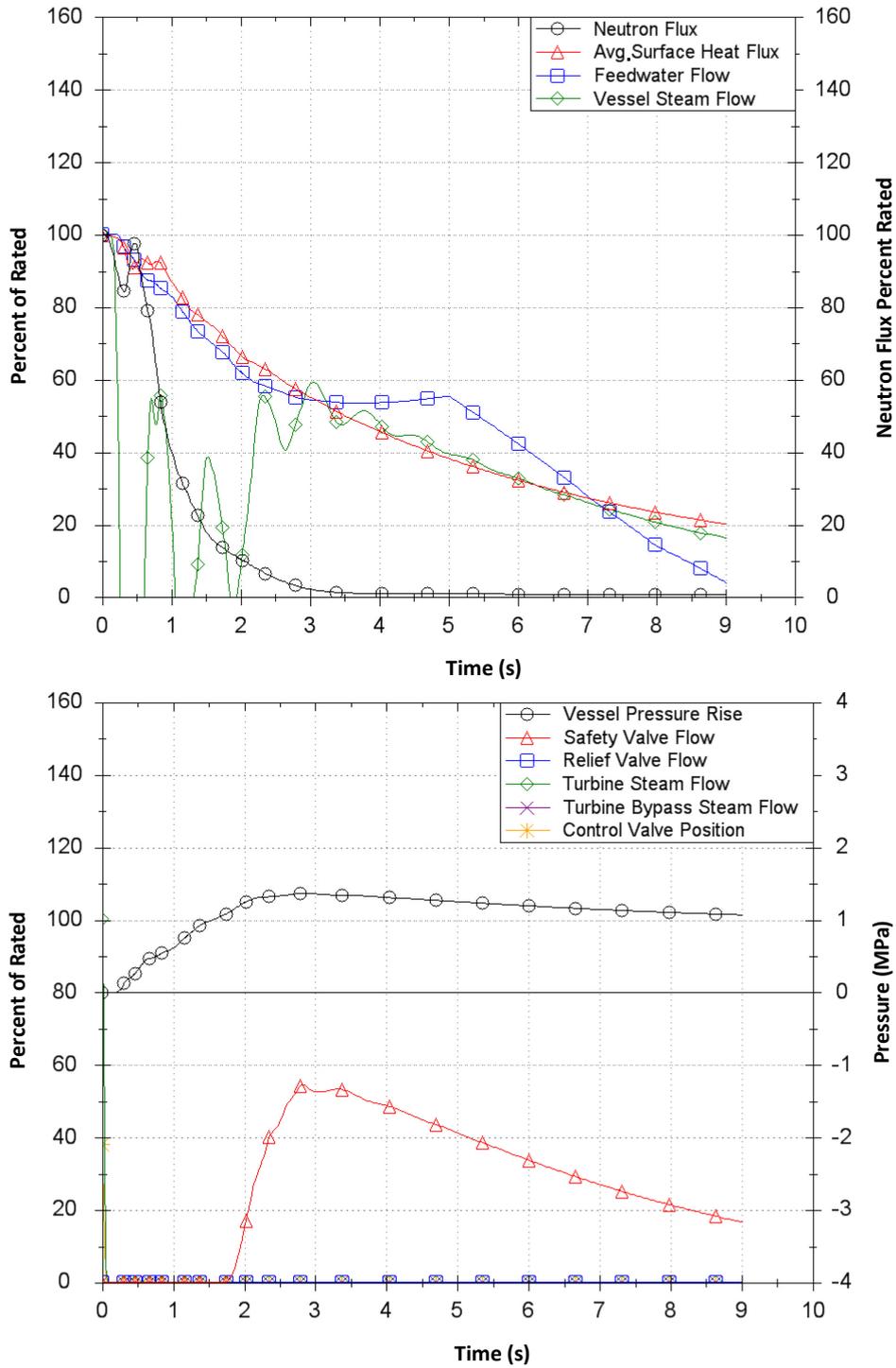


Figure 24.7.3-1: Loss of Off-site Power

24. Design Basis Analysis
24.7 Analysis Results and Fault-based View – Isolation Events
Ver. 0

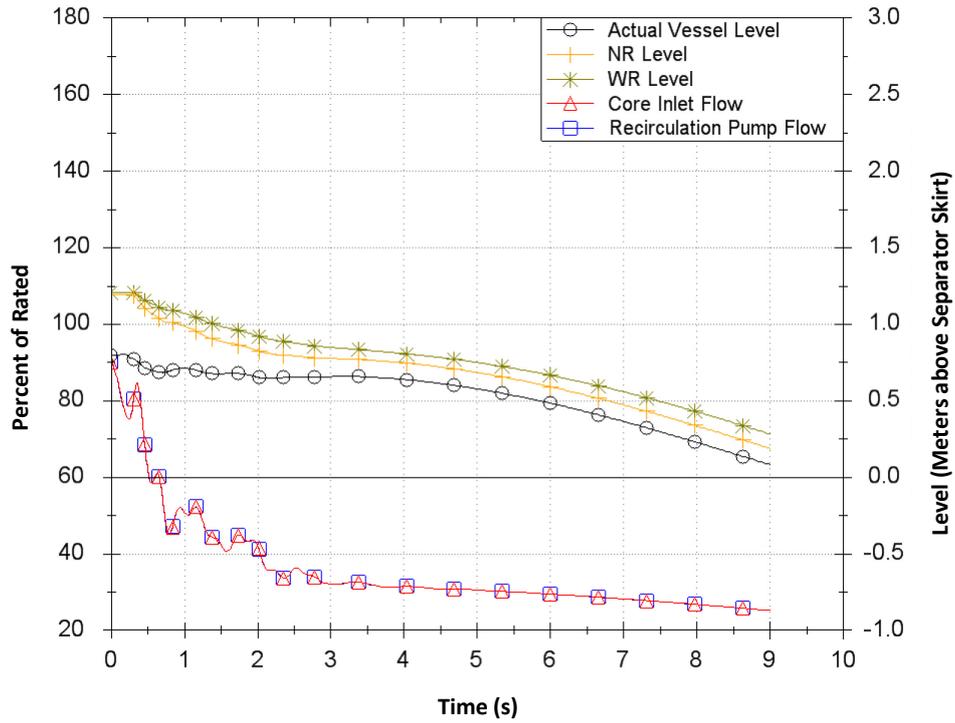


Figure 24.7.3-1: Loss of Off-site Power (Continued)

24.8 Analysis Results and Fault-based View – Loss of Coolant Events

This section shows the analysis for a number of Loss of Coolant Accidents (LOCAs):

- Inadvertent opening of SRV – see Section 24.8.1
- Small LOCA inside primary containment (bounded by Medium LOCA inside containment)
- Medium LOCA inside primary containment – see Section 24.8.2
- Large LOCA inside primary containment – see Section 24.8.3
- LOCA outside primary containment – see Section 24.8.4

Inadvertent opening of a SRV is the result of the mechanical failure of a valve (Class1) or inadvertent opening through the Class 1 SSLC or Class 2 HWBS either automatically or as a result of operator error. All of the other LOCA events are the result of failures of pipework.

The classification of the relevant pipework is discussed in Chapter 8: Structural Integrity. Chapter 8 also discusses the materials, manufacturing and failure mechanisms relevant to failures leading to LOCA events and the estimation of their frequency. As a general rule, pipework is Class 1 whilst it is inside the primary containment. However, as the pipe run leaves the primary containment it may have a lower class depending on the consequences of its failure. The class of each section of pipe determines the codes and standards under which it is manufactured, installed and inspected.

Provision of HLSFs is mainly the same as for the events described in Section 24.6 and 24.7. For LOCAs, the main consideration is the provision of water to ensure that the fuel cladding is protected from loss of one barrier to release primary circuit activity. In the UK ABWR design, this function is supplied by the Emergency Core Cooling System as shown in HLSF 2-1 of Table 24.8-1.

The general strategy for LOCAs is to scram the reactor and then provide water at a high pressure initially using HPCF and/or RCIC. As the pressure decreases, injection is switched to LPFL, which is a function of RHR. As the pressure approaches cold shutdown conditions, at least one of the RHR heat exchangers can be used and the reactor brought to cold shutdown.

In addition, the UK ABWR has Passive Auto-catalytic Recombiners (PARs) as part of the Flammability Control System (FCS) to protect against unacceptably high concentration of flammable gases in the PCV. The secondary containment is provided to confine and collect radioactive substances which may leak from the primary containment following a LOCA. This collection allows effective filtration by the Standby Gas Treatment System (SGTS) prior to release to the environment. The secondary containment region completely surrounds the PCV. These SCCs are shown in Table 24.8-2.

Table 24.8-1: Provision of HLSFs by Class 1 Systems for LOCA

HLSF	System	PCSR reference	Notes
1-3 Emergency shutdown of the reactor	CRD	11.5.2, 12.4.3.1	The corresponding setpoints are shown in Table 24.6-3.
2-1 Functions to cool reactor core	RCIC HPCF LPFL ADS or Transient ADS	13.4	LPFL is a function of RHR. ADS (for LOCA inside PCV) or Transient ADS (for LOCA outside PCV) depressurise reactor so that LPFL can inject. Power for ECCS, except for RCIC, is provided by EDG.
3-1 Functions to remove residual heat after shutdown	RHR	12.3.5.4	Power for RHR is provided by EDG. Heat is rejected to RCW and RSW
4-7 Functions to confine radioactive materials, shield radiation, and reduce radioactive release	PCV PCIS	13.3.3.1 13.3.3.2	PCV and PCIS limit leakage of radioactive materials in a LOCA.
	MSIV	12.3.5.2	MSIV is closed to form a barrier to confine radioactive materials within PCV in a LOCA inside PCV or to isolate the reactor in the event of MS line break outside PCV.
	Flow restrictor	12.3.5.2	Flow restrictor limits the steam flow in the event of MS line break.
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SSLC	14.6.2.1	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system.
5-2 Supporting functions especially important to safety	Class 1 EPS	15.3	Class 1 EPS supplies power to Class 1 SSCs. EDG supports SSCs related to HPCF and RHR (LPFL).
	RCW/RSW	16.3.2	RCW/RSW are essential systems for supporting HPCF, RHR and Class 1 HVAC operations.
	UHS	16.3.1	UHS provides sufficient cooling water to the RSW.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 1 HVAC	16.5	Class 1 HVAC ensures the adequate environmental parameters for Class 1 SSCs are maintained.
	HECW	16.3.5.1	HECW provides chilled water for Class 1 HVAC.

Table 24.8-2: Provision of HLSFs by Lower Class Systems for LOCA inside Primary Containment

HLSF	System	PCSR reference	Notes
4-7 Functions to confine radioactive materials, shield radiation, and reduce radioactive release	Secondary Containment (Class2)	13.3.4.1	Radioactive materials leaked from the PCV are collected within Secondary Containment and treated before release to the environment by SGTS.
	R/A HVAC isolation damper (Class 2)	16.5	R/A HVAC isolation damper is closed to form Secondary Containment.
	SGTS (Class 2)	13.3.4.2	SGTS controls the emission of radioactive materials by maintaining a negative pressure in the Secondary Containment and by filtering the effluent prior to discharge to the atmosphere following a LOCA.
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SACS (Class 2)	14.6.4	SACS provides the functions to generate actuation signals for SSCs related to SGTS.
5-15 Functions to control hydrogen concentration in accident conditions	FCS (Class 2)	13.3.3.3	FCS consists of PARs and controls flammable gas concentration in the PCV. Hydrogen and oxygen in the PCV are recombined by PARs.

Limits and Conditions for Operation

The following LCO is identified in addition to those in Section 24.6 and Section 24.7:

The future licensee shall ensure that, during normal power operation, one or more divisions of the following systems are operational even if one division is unavailable due to testing or maintenance and another division is unavailable due to a single failure:

- LPFL

The future licensee shall ensure that, during normal power operation, the following SSCs are operational:

- ADS

- Transient ADS
- PCV
- PCIS
- Secondary Containment
- R/A HVAC isolation damper
- SGTS
- SACS
- FCS (PARs)

The future licensee shall ensure that, during normal power operation, the reactor coolant circuit activity is below the DB Primary Source Term as defined in Chapter 20.

24.8.1 Inadvertent Opening of a SRV

Fault Schedule Ref: 6.1

In this section, the analysis of the Inadvertent Opening of a SRV event is presented.

(1) Description of Fault

The cause of the inadvertent opening of the SRV is attributed to malfunction of the valve or an operator initiated opening (operator error). Discharge from the SRV is to the Suppression Pool which condenses the steam and removes radioactive material carried over with the steam. The event does not bound any other events and is assumed to be a frequent fault because it can be caused by human error.

(2) Plant Normal Response

EHC (Class 3) would control the reactor pressure and all protections would be initiated automatically, which is the same as the analysis shown in this section.

(3) Analysis of Event

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (vii) below. Further details of the analysis conditions are described in A.5.5.1.1 in Topic Report on DBA [Ref-5].

- (i) The initial conditions of this analysis are shown in Table 24.6-2.
- (ii) It is assumed that the opening of one SRV allows steam to be discharged into the suppression pool.
- (iii) The initial core flow is assumed to be 90%, as a representative case, since it has no effect on the comparisons of the results against the acceptance criteria.
- (iv) The operating mode of the RFC (Class 3) is assumed to be manual (frozen).
- (v) The EHC (Class 3) is assumed to be working.
- (vi) The FDWC (Class 3) is assumed to be working.
- (vii) One division of ECCS is assumed to be available.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

AC-F1: The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.

AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

AC-D1: Dose to workers should be less than 20 mSv.

AC-D2: Dose to members of the public should be less than 1 mSv.

(c) Fault Progression

The opening of one SRV allows steam to be discharged into the suppression pool. The sudden increase in the rate of steam flow leaving the reactor vessel causes a mild depressurisation transient. The EHC senses the nuclear system pressure decrease and within a few seconds closes the TCVs far enough to stabilise the reactor vessel pressure at a slightly lower value and the reactor settles at nearly the initial power level. Thermal margins decrease only slightly through the transient and no fuel damage results from the transient. The MCPR is essentially unchanged and, therefore, the safety limit margin is unaffected and this event does not have to be reanalysed for specific core configurations.

(d) Analysis Results

The result of the Inadvertent Opening of an SRV is shown in Table 24.8-3 and Figure 24.8.1-1.

The results are compared with the acceptance criteria described above as follows:

- The Δ CPR is negligible, and so the MCPR remains above the safety limit MCPR (1.06). (AC-F1 met with significant margin)
- The surface heat flux does not exceed the initial value. (AC-F2 met with significant margin)
- The peak pressure on the reactor coolant pressure boundary is 7.28 MPa [gauge], and so it does not exceed the acceptance criterion 9.48 MPa [gauge]. (AC-R1 met with significant margin)
- Pressure on the primary containment boundary does not exceed the maximum allowable working pressure since the enthalpy released to the suppression pool via the open SRV is low enough to be removed by the heat removal systems such as the RHR. (AC-C1 met with significant margin)

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met with significant margins.

The margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

Table 24.8-3: Results Summary for Inadvertent Opening of an SRV

Figure ID	Max. Neutron Flux (% NBR)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Core Average Surface Heat Flux (% of Initial)	Δ CPR
Figure 24.8.1-1	100	7.28	100	Note 1

(Note) 1: Not limiting for Δ CPR

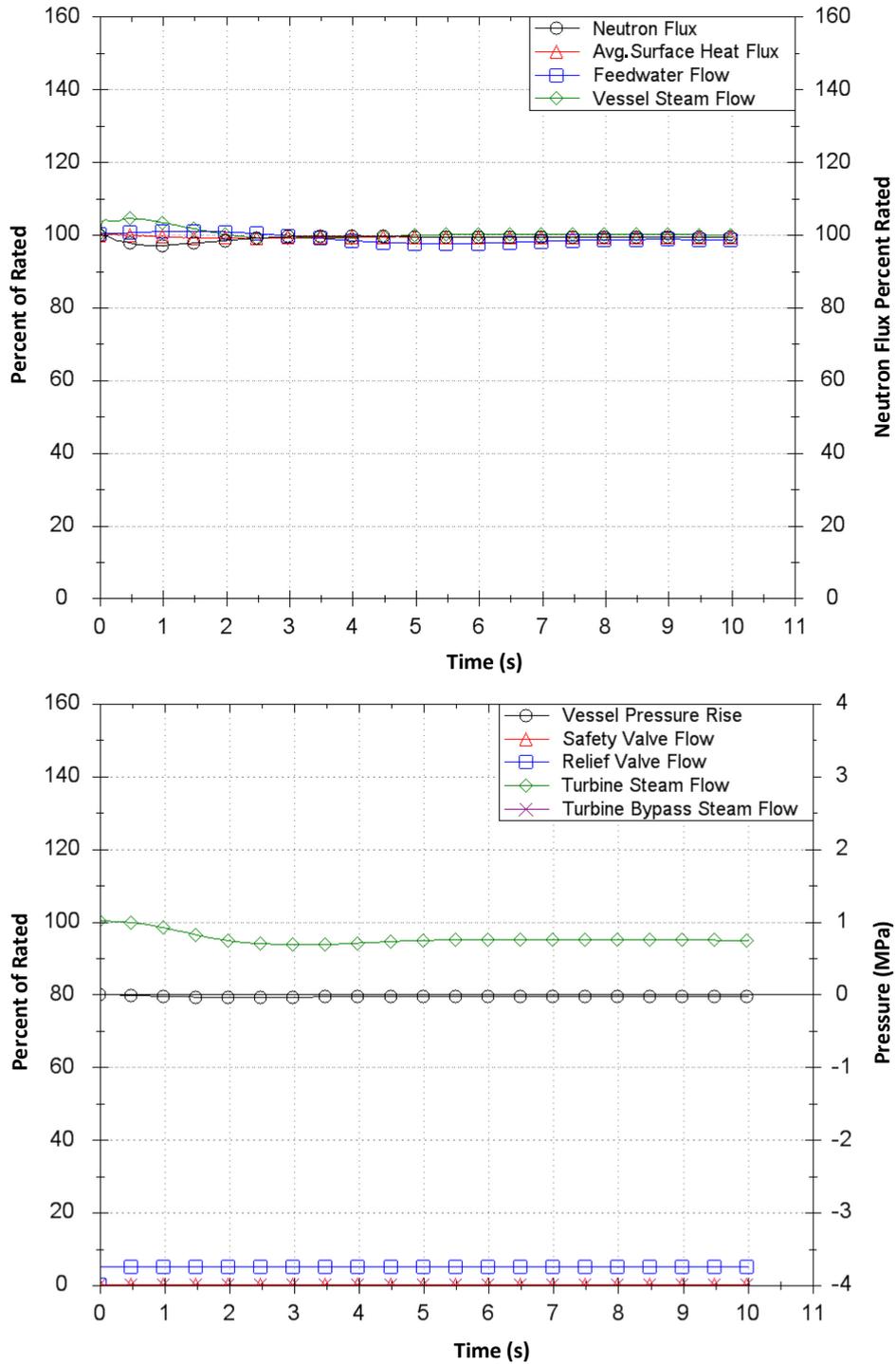


Figure 24.8.1-1: Inadvertent Opening of an SRV

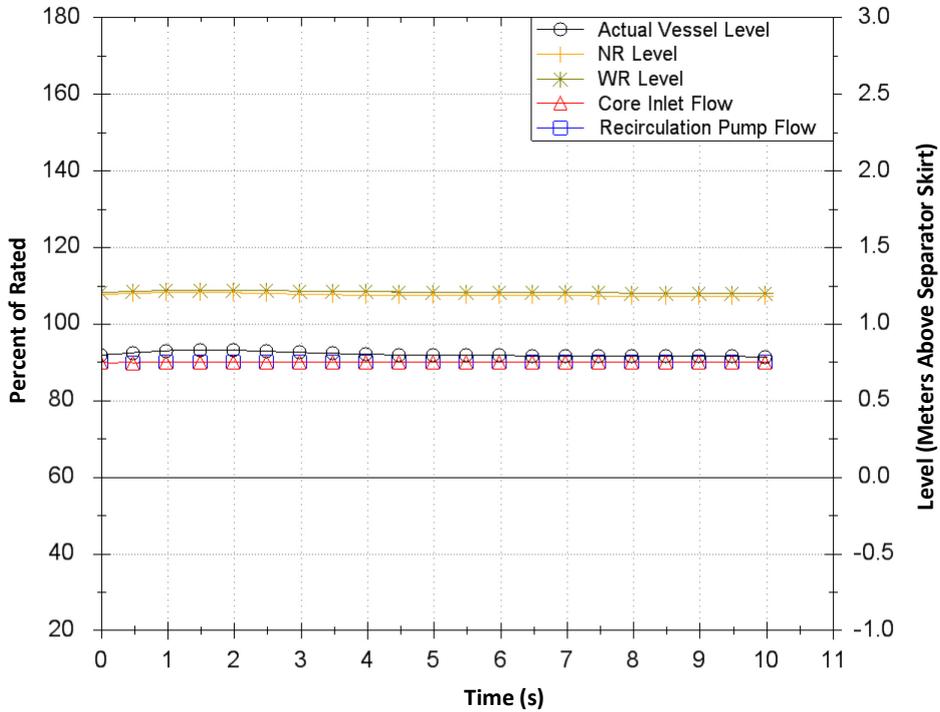


Figure 24.8.1-1: Inadvertent Opening of an SRV (Continued)

24.8.2 Medium LOCA inside Primary Containmentment

The reactor pressure boundary consists of the RPV, main steam and feedwater piping and a number of smaller pipes. For a medium LOCA, one of these pipes is assumed to break, leading to coolant being discharged into the Primary Containmentment Vessel (PCV). If the coolant lost is not replaced, the reactor core could become uncovered and fuel might be damaged because of insufficient cooling.

The following cases are in or bounded by the Medium LOCA inside Primary Containmentment fault group:

- Small LOCA inside Primary Containmentment
 - RPV bottom drain line break (Fault Schedule Ref: 7.1)
 - Small line break LOCA (Fault Schedule Ref: 7.2)
- Medium LOCA inside Primary Containmentment
 - High Pressure Core Flooder System line break (Fault Schedule Ref: 8.1)
 - Low Pressure Flooder System line break (Fault Schedule Ref: 8.2)

For all piping breaks in the UK ABWR, Peak Cladding Temperature (PCT) is almost the same value, and the inventory of the coolant reduces most for a HPCF piping break. Therefore, the HPCF piping break is the bounding fault.

The analyses conditions for LOCA events are given in Table 24.8-4.

Table 24.8-4: Main Analysis Conditions for LOCA

Items	Values
Reactor thermal power	About 102% of the rated power (4005 MW)
Peak linear heat generation rate	44.0 kW/m × 1.02
Core flow	100% of the rated flow rate (52.2 × 10 ³ t/h)
Reactor pressure	7.17 MPa [gauge]
Core inlet enthalpy	1.23 MJ/kg
High Pressure Core Flooder System flow (rated value)	727 m ³ /h (at 0.689 MPa[dif] per pump)*
Low Pressure Flooder System flow (rated value)	954 m ³ /h (at 0.276 MPa[dif] per pump)*
Reactor Core Isolation Cooling System flow (rated value)	182 m ³ /h (at 8.115 to 1.034 MPa[dif] per pump)*
Setpoints for low reactor water level (main steam isolation valve closing, and HPCF, RCIC (ECCS function) and emergency diesel generator (divisions II and III) starting)	Level 1.5
Setpoints for low reactor water level (LPFL, emergency diesel generator (division I) and Automatic Depressurisation System (ADS) starting)	Level 1
Primary circuit activity levels are below those in Primary Source Term	The DB Primary Source Term (PST) is defined in Chapter 20.

*: MPa[dif] : differential pressure between the reactor pressure vessel and water source

24.8.2.1 HPCF Line Break

Fault Schedule Ref: 8.1

(1) Description of Fault

In this fault, the HPCF line is assumed to fail inside the primary containment leading to reactor coolant being discharged inside the PCV. This is an infrequent fault.

The fault is protected against by the ECCS as listed in Table 24.8-1.

(2) Plant Normal Response

The plant normal response to this event is to automatically scram the reactor and initiate ECCS as in the fault analysis.

(3) Analysis of Event

The analysis results produced by the computer codes are presented in detail as follows. The analysis is divided into two parts:

- Single failure assumption
- Combination of maintenance unavailability and a single failure

(I) Single failure assumption

(a) Analysis Assumptions

The following analysis conditions are assumed.

- (i) The analysis conditions are as shown in Table 24.8-4.
- (ii) For gap conductance between the fuel cladding and pellet, a value to make the analysis result conservative is used in consideration of variations during the exposure (fuel burnup) cycle.
- (iii) For decay heat after shutdown of the reactor, 1.2 times the values of 1971 ANS Standard are used.
- (iv) It is assumed that off-site power is lost concurrently with the occurrence of the accident and that all 10 RIPs trip simultaneously.
- (v) Though the reactor water level is maintained above Level 4, it is assumed that the initial water level is at low reactor water level (Level 3) to conservatively reduce the inventory of the coolant. Reactor scram is initiated concurrently with the occurrence of the accident.
- (vi) It is assumed that the signal for high drywell pressure as an ECCS start-up signal is given

earlier than the signal for low reactor water level (Level 1.5 or 1), however, ECCS is conservatively assumed to start up on the signal for low reactor water level.

- (vii) The most conservative single failure is assumed in the ECCS network from the viewpoint of its impact on reactor cooling capability. The most conservative single failure in the case of the HPCF pipe break accident is a failure of an emergency diesel generator that supplies power to the intact HPCF.
- (viii) The leakage of coolant from the break is calculated based on the homogeneous critical flow model.
- (ix) The opening pressures of the safety relief valves are 1.03 times higher than the setpoint values to allow for setting errors.
- (x) For heat transfer coefficient between the fuel cladding and the coolant in the calculation of the fuel cladding temperature, the following correlations are used:
 - Nucleate boiling cooling: correlation used as a function of the void fraction
 - Film boiling cooling: mist cooling correlation and the Modified Bromley correlation used as functions of the void fraction
 - Transition boiling cooling: correlation in which heat transfer coefficients of nucleate boiling and film boiling are interpolated with the fuel cladding superheat
 - Steam cooling: Dittus-Boelter correlation
 - Mist cooling: Dittus-Boelter correlation and dispersed droplet flow film boiling
- (xi) The volume of oxidation of fuel cladding produced by zirconium-water reaction is calculated using the Baker-Just equation.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

It is noted that the acceptance criteria relating to fuel are used for this analysis. The acceptance criteria related to containment and dose for loss of cooling events are confirmed by analysis of the Feedwater line break inside containment, this being the limiting fault for these criteria as indicated in Section 24.8.3.1.

(c) Fault Progression

Following the postulated break of a HPCF line, the fault progresses as follows:

- (i) Instantaneous double-ended break of piping, and reactor scram on low reactor water level (Level 3)
- (ii) Discharge of coolant from the RPV to the PCV (Blowdown phase)
- (iii) Decrease in RPV pressure, inventory and core flow rate
- (iv) Full closure of the MSIVs (Level 1.5)
- (v) Start of coolant injection by the RCIC on low reactor water level (Level 1.5)
- (vi) Actuation of ADS on low reactor water level (Level 1) and high drywell pressure with a 30s delay
- (vii) Start of coolant injection by the LPFL on low reactor water level (Level 1)
- (viii) Recovery of water level inside the core shroud

During the blowdown phase, heat transfer from the fuel to the coolant undergoes a boiling transition from nucleate boiling (normal conditions) to film boiling.

(d) Analysis Results

(i) Responses of core flow, reactor pressure, reactor water level and fuel cladding temperature

After the occurrence of the double-ended break of a HPCF line, critical flow occurs at the HPCF sparger nozzle which has the smallest area within the flow path from the HPCF sparger to the break.

Because of the assumption of loss of off-site power occurring concurrently with the accident, core flow rapidly decreases because of the trip of the recirculation pumps.

Due to the rapid decrease of core flow, MCPR falls below the Safety Limit MCPR value at about 1 second after the accident and boiling transition occurs as far as the fourth spacer position from the top of the fuel assembly. Consequently, the heat transfer coefficient from fuel cladding to coolant decreases and the fuel cladding temperature increases. However, the increase of fuel cladding temperature stops after a short time because of the decrease of power due to the reactor scram.

On the other hand, the water level inside the core shroud starts to decrease. However, the RCIC is activated by a low reactor water level (Level 1.5) signal and starts water injection at about 95 seconds after the accident. ADS is also activated to lower the reactor pressure by a high drywell pressure signal and a low reactor water level (Level 1) signal at about 171 seconds

after the accident. Two LPFL pumps are actuated by a low reactor water level (Level 1) signal to inject water at about 357 seconds. The water level inside the core shroud does not decrease below the top of the active fuel, and the core is kept flooded. Therefore, temperature increase of the fuel cladding because of core uncovering does not occur. The peak fuel cladding temperature occurs during the boiling transition immediately after the accident.

Figure 24.8.2-1 shows the reactor water level transient and Figure 24.8.2-2 shows the reactor pressure transient during the accident. Figure 24.8.2-3 shows the heat transfer coefficient transient at the position of maximum fuel cladding temperature, and Figure 24.8.2-4 shows the fuel cladding temperature transient. The peak fuel cladding temperature during the accident is about 641 °C.

(ii) Perforation and oxidation of fuel cladding

Fuel rods can be perforated when the fuel cladding temperature increases after an accident if the hoop stress due to internal pressure exceeds the perforation stress at that temperature.

The peak fuel cladding temperature reached during this bounding LOCA is about 641 °C. The calculated hoop stress is less than the value at which fuel cladding is perforated. Therefore, fuel rods are not perforated during a LOCA.

Increase of oxide layer thickness on the fuel cladding is very small because the fuel cladding temperature is relatively low.

(iii) Summary of analysis results

The water level inside the core shroud does not fall below the top of the active fuel – the fuel remains covered during the accident. The peak cladding temperature is around 641 °C and so the cladding temperature remains much lower than the value of 1200 °C to meet the infrequent fault acceptance criterion. (AC-F5 met with significant margin)

The increase in cladding oxide layer is very small, and much less than the 15% limit of the acceptance criterion. (AC-F4 met with significant margin)

The peak cladding temperature and the peak hoop stress are less than the value for perforation of the fuel cladding. Therefore there is no fuel rupture.

(II) Combination of maintenance unavailability and a single failure**(a) Analysis Assumptions**

The worst case assumption for the HPCF pipe break is the unavailability of the EDG providing power to the other HPCF division plus single failure of the RCIC.

The other conditions are the same as those shown in item (a) of subsection (I) above, except for item (vii).

(b) Fault Progression

Fault progression is the same as shown in item (c) of subsection (I) above, except for item (v). Although the reactor water level is lower than the Top of Active Fuel (TAF) for a very short time, the PCT remains much lower than 1200 °C.

(c) Analysis Results

The reactor water level decreases much more compared to the case with only the single failure assumption because there is no RCIC injection in this case, and the water level is lower than the TAF for a very short time. The ADS is actuated by a high drywell pressure signal and a low reactor water level (Level 1) signal at about 163 seconds after the accident. One LPFL pump is actuated by a low reactor water level (Level 1) signal to inject water at about 357 seconds. The reactor water level recovers because of LPFL injection. Although the water level is lower than the TAF for a very short time, the cladding temperature due to core heatup is less than that occurs earlier during boiling transition. Thus, the peak cladding temperature is unchanged from case (i) above at around 641 °C and so the cladding temperature remains much lower than the criterion value of 1200 °C to meet the acceptance criterion. (AC-F5 met with significant margin)

Figure 24.8.2-5 shows the reactor water level transient and Figure 24.8.2-6 shows the reactor pressure transient during the accident. Figure 24.8.2-7 shows the fuel cladding temperature transient.

The increase in cladding oxide layer is very small because the fuel cladding temperature is relatively low, and it is much less than the 15% to meet the acceptance criterion. (AC-F4 met with significant margin)

The peak cladding temperature and the peak hoop stress are less than the value for perforation of the fuel cladding. Therefore there is no fuel rupture.

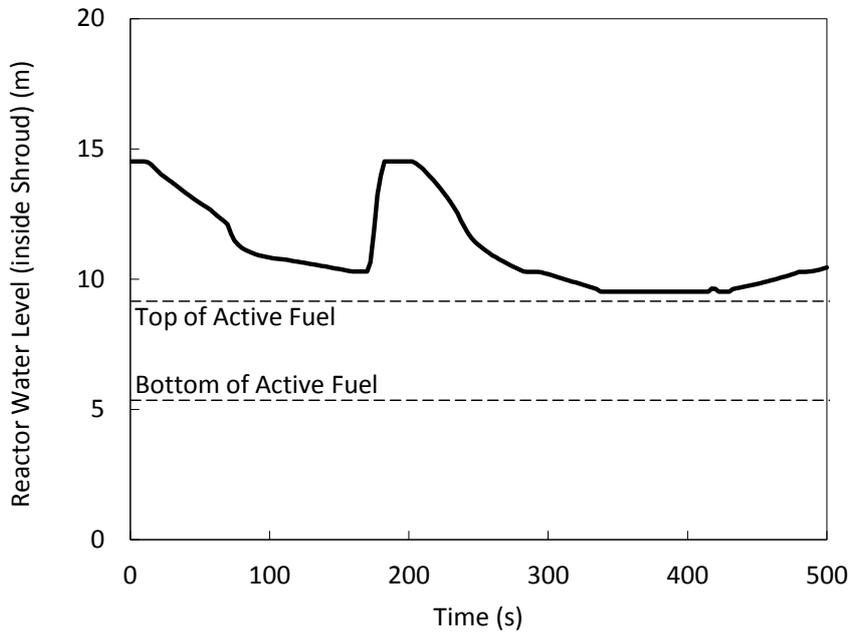


Figure 24.8.2-1: Reactor Water Level during HPCF Line Break (with RCIC and two LPFLs)

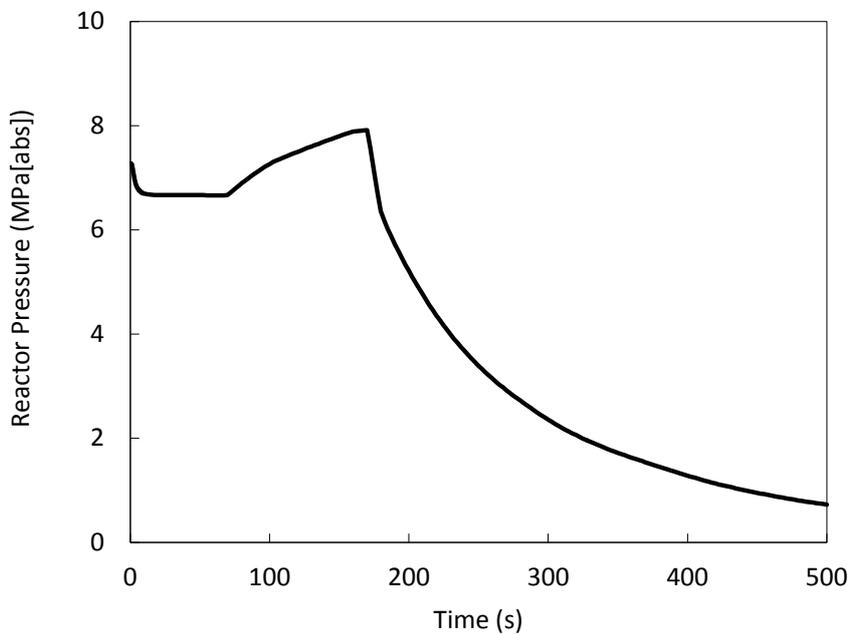


Figure 24.8.2-2: Reactor Pressure during HPCF Line Break (with RCIC and two LPFLs)

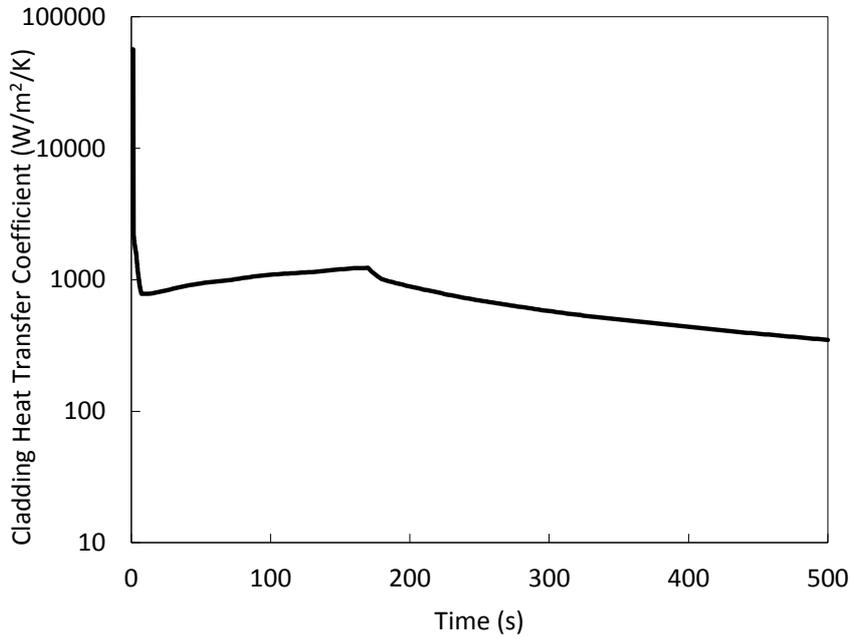


Figure 24.8.2-3: Heat Transfer Coefficient at the Maximum Fuel Cladding Temperature Position during HPCF Line Break (with RCIC and two LPFLs)

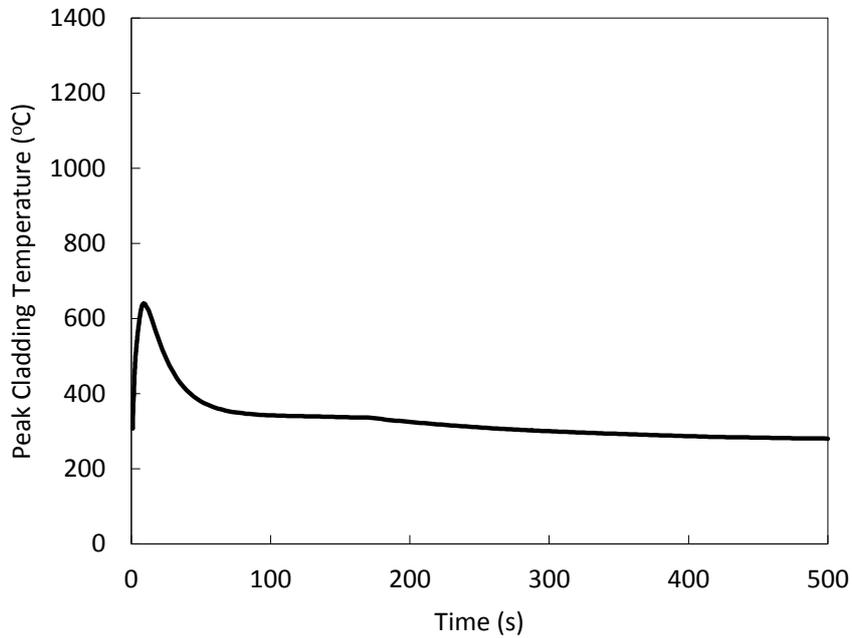


Figure 24.8.2-4: Peak Cladding Temperature during HPCF Line Break (with RCIC and two LPFLs)

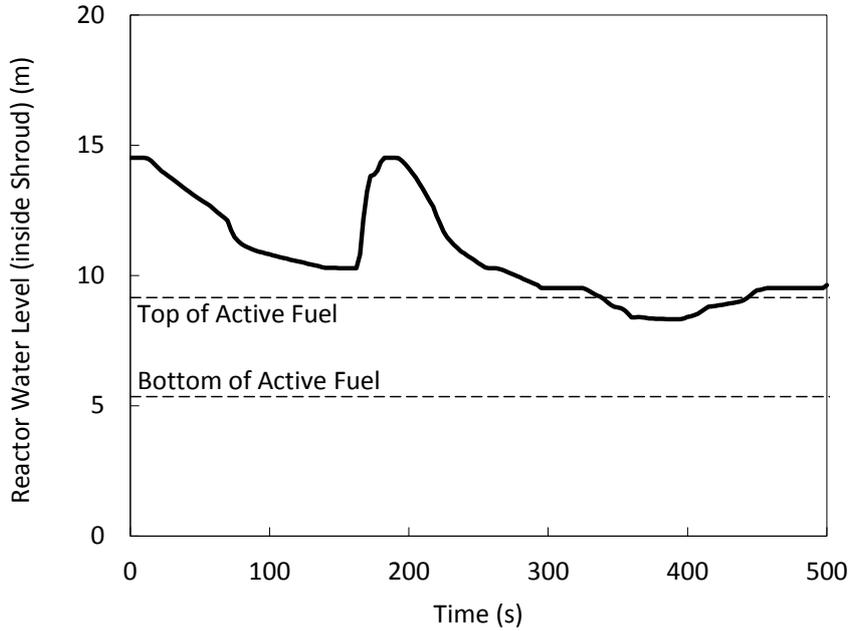


Figure 24.8.2-5: Reactor Water Level during HPCF Line Break (with one LPFL)

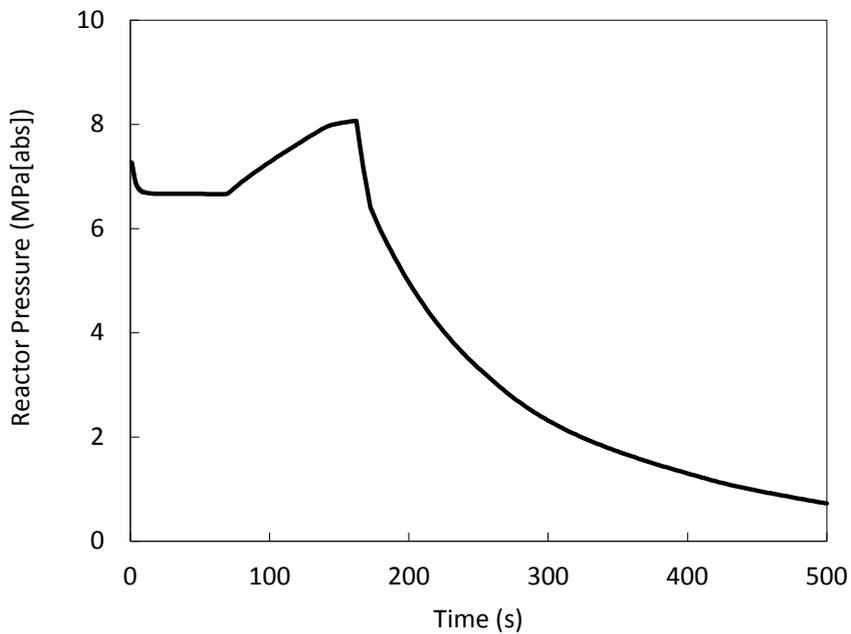


Figure 24.8.2-6: Reactor Pressure during HPCF Line Break (with one LPFL)

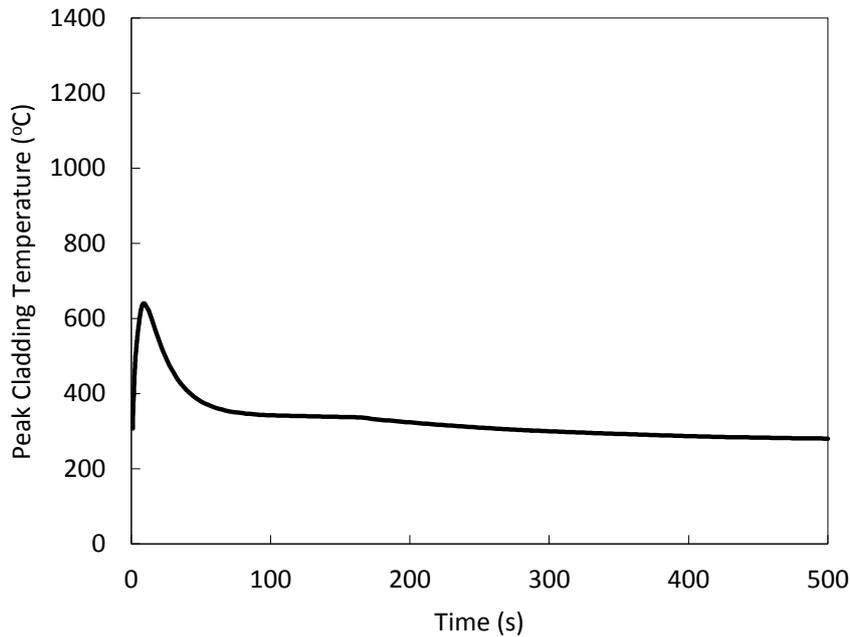


Figure 24.8.2-7: Peak Cladding Temperature during HPCF Line Break (with one LPFL)

(4) Discussion and Conclusions

In the cases analysed, the increase in cladding oxide layer is very small because the fuel cladding temperature is relatively low, and it is much less than the 15% to meet the acceptance criterion. Further, the peak cladding temperature and the peak hoop stress are significantly less than the value for perforation of the fuel cladding. Therefore there is no fuel rupture and the margins before fuel failure are large.

In addition, should there be a failure of injection functions, initiation of FLSS, either automatically or manually, provides resilience of protection against this fault. No further reasonably practicable means of protection have been identified and the risks from this fault are deemed to be ALARP.

24.8.3 Large LOCA inside Primary Containment

The following cases are in the Large LOCA fault group:

- Feedwater line break (FWLB) (Fault Schedule Ref: 9.1)
- Main steam line break (MSLB) (Fault Schedule Ref: 9.2)
- Residual Heat Removal System outlet line break (Fault Schedule Ref: 9.3)

For the evaluation of PCV integrity during a LOCA, the feedwater line break inside primary containment is the bounding fault for PCV pressure and the main steam line break inside primary containment is the bounding fault for PCV temperature. It is noted that the HPCF line break presented in Section 24.8.2.1 is the bounding fault for fuel integrity.

The analysis conditions for Large LOCA inside primary containment are given in Table 24.8-5.

Table 24.8-5: Main Analysis Conditions for Feedwater Line Break / Main Steam Line Break inside Containment

No.	Item	Analysis Condition	Remark
1	Reactor thermal power	4005 MW (102% of rated power)	
2	Blowdown model	Moody's theory	
3	Decay Heat	ANSI/ANS-5.1	
4	PCV volume (1) Drywell (2) Suppression Chamber (3) Suppression Pool Water	7350 m ³ 5960 m ³ 3580 m ³	
5	Initial Pressure (1) Drywell (2) Suppression Chamber	9 kPa [gauge] 9 kPa [gauge]	
6	Initial Temperature (1) Drywell (2) Suppression Chamber	57 °C 35 °C	
7	Initial Humidity (1) Drywell (2) Suppression Chamber	20% 100%	
8	Vent Pipes (1) Flow Area (2) Submergence	11.3 m ² 3.6 m	
9	Start time of PCV Spray	N/A	PCV spray is not used.
10	RHR Heat Exchanger Capacity	5.88×10^5 W/K/unit	It is assumed that heat removal by the RHR heat exchanger becomes available 30 minutes after the accident
11	RHR Heat Exchanger Water Supply Temperature	30 °C	
12	Pump Heat	5000 kW	All of ECCS pump heat is considered.
13	Combination of maintenance unavailability and a single failure	EDG division II EDG division III	
14	Operation of ECCS (1) Before PCV cooling systems actuation (2) After PCV cooling systems actuation (3) Water Source	RCIC + LPFL (Core cooling) LPFL with heat exchanger (PCV cooling) (LPFL)* Suppression Pool	It is assumed that only one division (division I) of ECCS is available. (ADS, RCIC and one division of the RHR system are available). *PCV is cooled by overflow of ECCS water from the RPV.
15	Vacuum Breaker Actuation pressure	3.4 kPa [dif]	

Limits and Conditions for Operation

The following LCO is identified in addition to those in Section 24.6, Section 24.7 and Section 24.8:

The future licensee shall ensure that, during normal power operation, the following plant conditions are maintained:

- Drywell pressure
- Drywell air temperature
- S/P average temperature
- S/P water level
- Oxygen concentration in the PCV

24.8.3.1 Feedwater Line Break / Main Steam Line Break inside Containment

Fault Schedule Ref: 9.1 and 9.2

(1) Description of Fault

In this fault, the feedwater line or the main steam line connected to the RPV is assumed to fail inside the primary containment leading to reactor coolant being discharged inside the PCV. This is an infrequent fault. This fault includes:

- Feedwater line break (FWLB) (Fault Schedule Ref: 9.1)
- Main steam line break (MSLB) (Fault Schedule Ref: 9.2)

(2) Plant Normal Response

The normal response of the plant to this fault is to automatically scram the reactor and initiate ECCS as in the fault analysis.

(3) Analysis of the Event

The analysis of this fault is presented in three parts:

- Analysis of the response of the PCV
- Analysis of concentration of flammable gas in PCV
- Dose evaluation

(I) PCV analysis

The response of the PCV during the short-term blowdown period of the accident and following the blowdown period (long-term) has been analysed respectively.

The maximum pressure and temperature in the Drywell (D/W) and Suppression Chamber (S/C) are calculated both in the short and long term.

(a) Analysis Assumptions

The analysis conditions are listed in (i) to (vii) below. Further details of the analysis conditions are described in Attachment D, section D.6 of the Topic Report on DBA [Ref-5].

- (i) Analysis conditions are as in Table 24.8-5.
- (ii) It is assumed that off-site power is lost simultaneously with the onset of the accident. Consequently, the recirculation pumps are tripped immediately.

- (iii) Moody's critical-flow model is used to calculate the flow of coolant from the break.
- (iv) Immediately before the onset of the accident, the Drywell (D/W) temperature is assumed to be 57 °C; the S/P water temperature is assumed to be 35 °C. These temperatures are in normal operating conditions. The pressure inside the containment vessel is assumed to be 9 kPa [gauge].
- (v) It is assumed that only one division (division I) of ECCS is available. (ADS, RCIC and one division of the RHR system are available).*
- (vi) It is assumed that heat removal by the RHR heat exchanger becomes available 30 minutes after the accident.*
- (vii) One division of ECCS is assumed to be available.*

*The ECCS is conservatively not modelled for the short term containment response analysis.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is an infrequent event, they are:

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

AC-D5: Dose to workers should be less than 500 mSv.

AC-D6: Dose to members of the public should be less than 100 mSv.

It is noted that the acceptance criteria relating to fuel are not used for this analysis because acceptance of AC-F5 and AC-F4 for loss of cooling events are confirmed by analysis of the HPCF line break being the limiting fault for these criteria, as indicated in Section 24.8.2.1.

(c) Fault Progression

When a double-ended break of the feedwater line occurs, the coolant flows out rapidly from the reactor and turbine side into the D/W and the D/W pressure increases.

For this reason, most of the gases inside the D/W are driven out by the outgoing flow of reactor coolant into the S/C, and the steam in the gases are condensed by the S/P water. On the other hand, the non-condensable gases will migrate to the airspace of the S/C, and the pressure in the S/C will rise.

After the water level in the RPV has been restored to the elevation of the feedwater lines due to the activation of the ECCS, the excess water will flow out through the break to the D/W. It cools and condenses the steam in the D/W and cause the heat generated in the core to move into the S/C. As a

result of condensation of the steam in the D/W, the D/W pressure decreases, and the vacuum breakers acts to redistribute the non-condensable gases in the S/C to the D/W and the S/C. The RHR System is used at first as a Low-Pressure Flooder System to refill the RPV without the heat exchanger. However, 30 minutes after the event, heat removal by the RHR heat exchanger becomes available.

After heat removal from the S/C by the RHR System has begun and the amount of heat generated from the core has become equal to the amount of heat removed by the cooling system, the temperature in the S/C starts to drop.

The temperature in the D/W and in the S/C drops as a result of the heat removal, and the pressure also falls along with this.

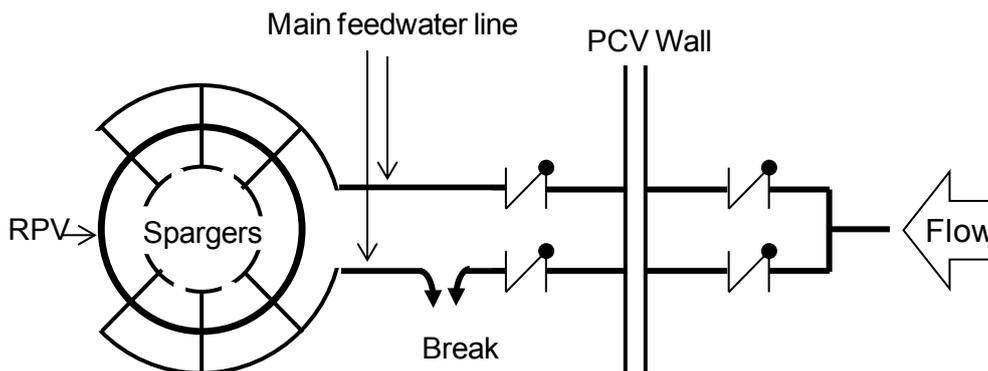


Figure 24.8.3-1: Break in a Feedwater Line inside Primary Containment

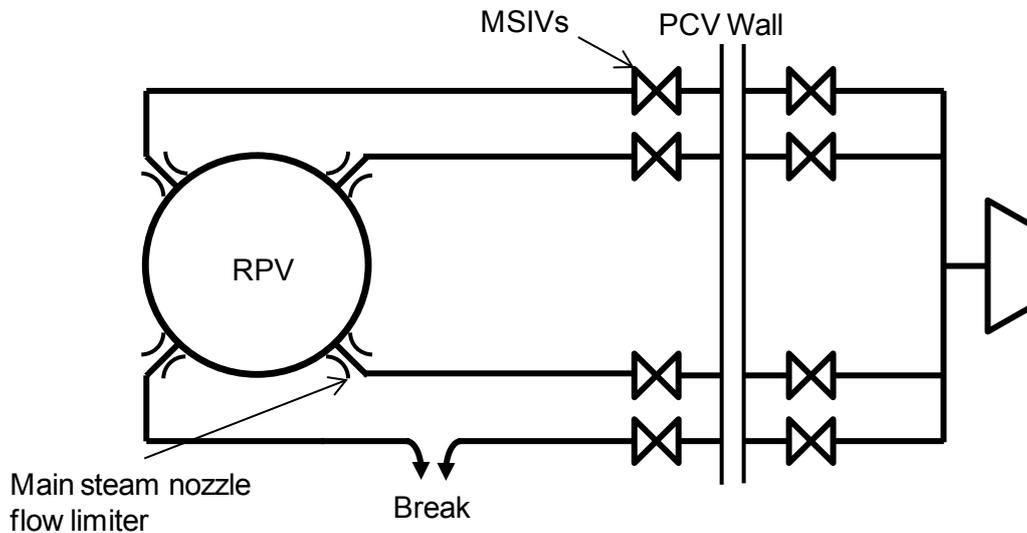


Figure 24.8.3-2: Break in a Main Steam Line inside Primary Containment

(d) Analysis Results

Figure 24.8.3-3 and Figure 24.8.3-4 show the results of short-term analysis of the pressure and temperature transients in the D/W and in the S/C after the FWLB accident. Figure 24.8.3-5 and Figure 24.8.3-6 show the results of long-term analysis of the pressure and temperature transients in the D/W and in the S/C after the FWLB accident.

Figure 24.8.3-7 and Figure 24.8.3-8 show the results of short-term analysis of the pressure and temperature transients in the D/W and in the S/C after the MSLB accident. Figure 24.8.3-9 and Figure 24.8.3-10 show the results of long-term analysis of the pressure and temperature transients in the D/W and in the S/C after the MSLB accident.

It is clear from these figures that the pressure inside the containment vessel reaches its maximum value of about 295 kPa [gauge] during the feedwater line break. This is lower than the design pressure of the containment vessel, which is 310 kPa [gauge], so AC-C1 is met. The activation of the RHR heat exchanger and overflow of ECCS water from the RPV enable the pressure and temperature in the containment vessel to be lowered.

The more severe case for temperature transient occurs during a main steam line break accident when the D/W airspace temperature and the S/P gas temperature reaches about 180 °C and 101 °C, respectively.

Although the calculated D/W airspace temperature exceeds the design limit of 171 °C, it stays at this high temperature for only a short time (about 1.1 seconds). This is acceptable because it takes a much longer time for the D/W structural materials to respond to the temperature rise, so the D/W structural materials remain below their design temperature.

The maximum S/P temperature of 100 °C also occurs during a main steam line break. This is below the design value of 104 °C.

The results summary for the large LOCA inside primary containment (PCV performance analysis) is shown in Table 24.8-7.

Table 24.8-6: Results Summary of PCV Performance Analysis

Design Parameter	Design Value	Calculated Value
1. Drywell pressure (kPa [gauge])	310	295
2. Drywell temperature (°C)	171	180* ¹
3. Wetwell pressure (kPa [gauge])	310	202
4. Wetwell temperature (°C)		
• Gas Space	104	101
• Suppression pool	104	100* ²

*¹ Although the calculated drywell airspace temperature exceeds the design limit, it does so for only a short time (about 1.1 seconds). Because it takes a much longer time for the drywell structural materials to respond to the temperature rise, the drywell structural materials remain below the design temperature.

*² Based on LOCA analysis (FWL and MSL breaks) corresponding to maximum service water temperature of 30 °C and pool initial temperature of 35 °C.

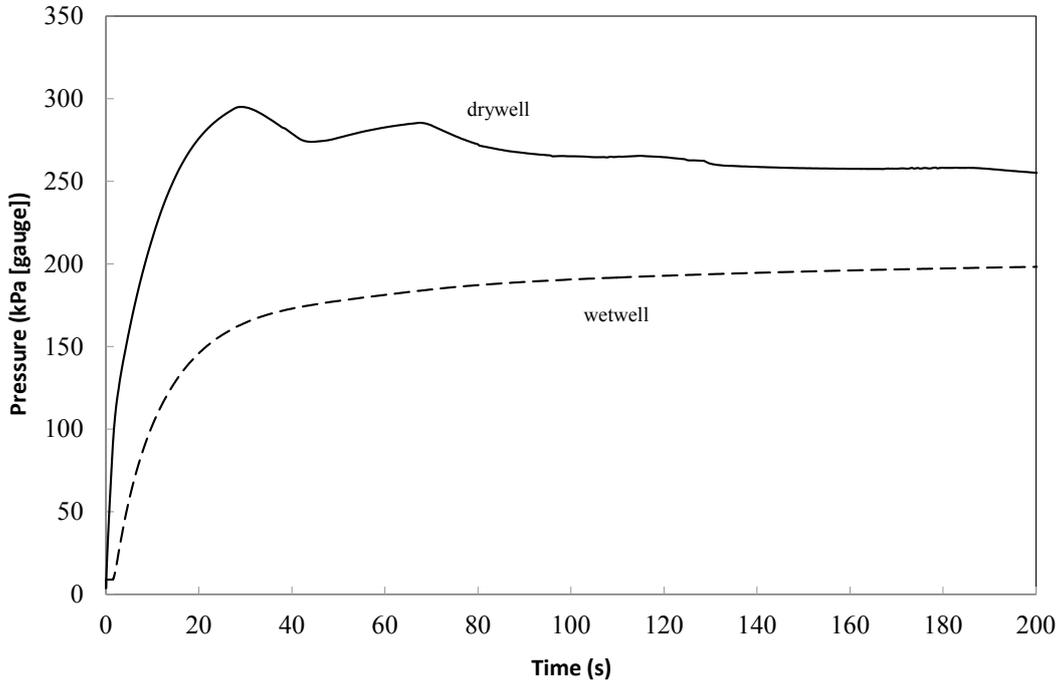


Figure 24.8.3-3: Pressure Transients in the D/W and S/C for Feedwater Line Break Accident (short-term)

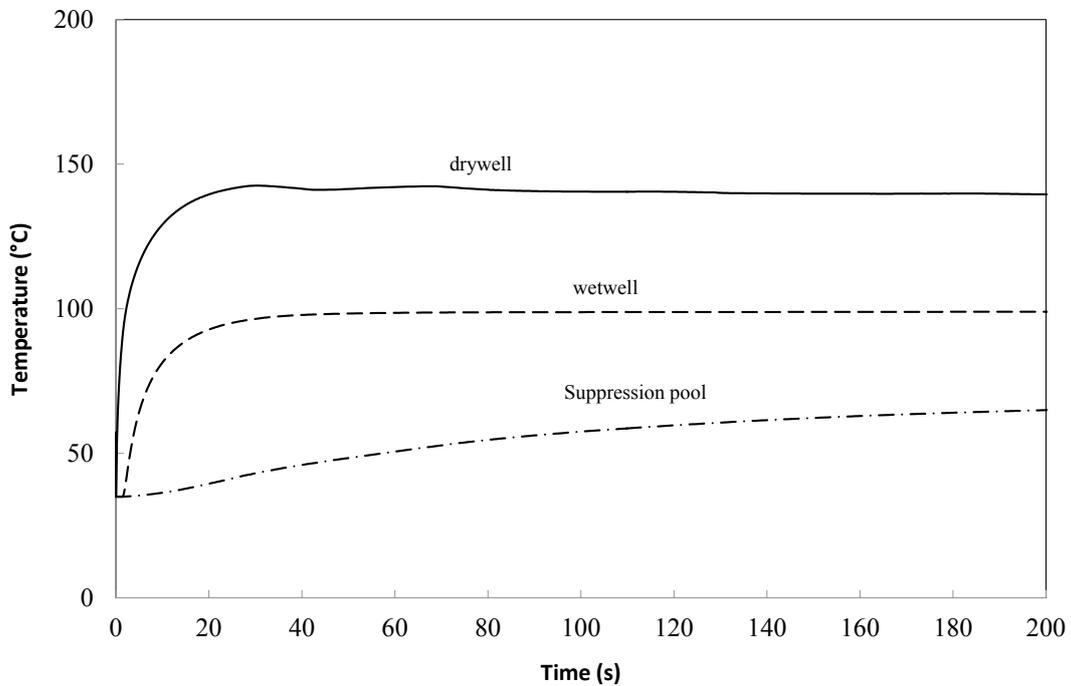


Figure 24.8.3-4: Temperature Transients in the D/W and S/C for Feedwater Line Break Accident (short-term)

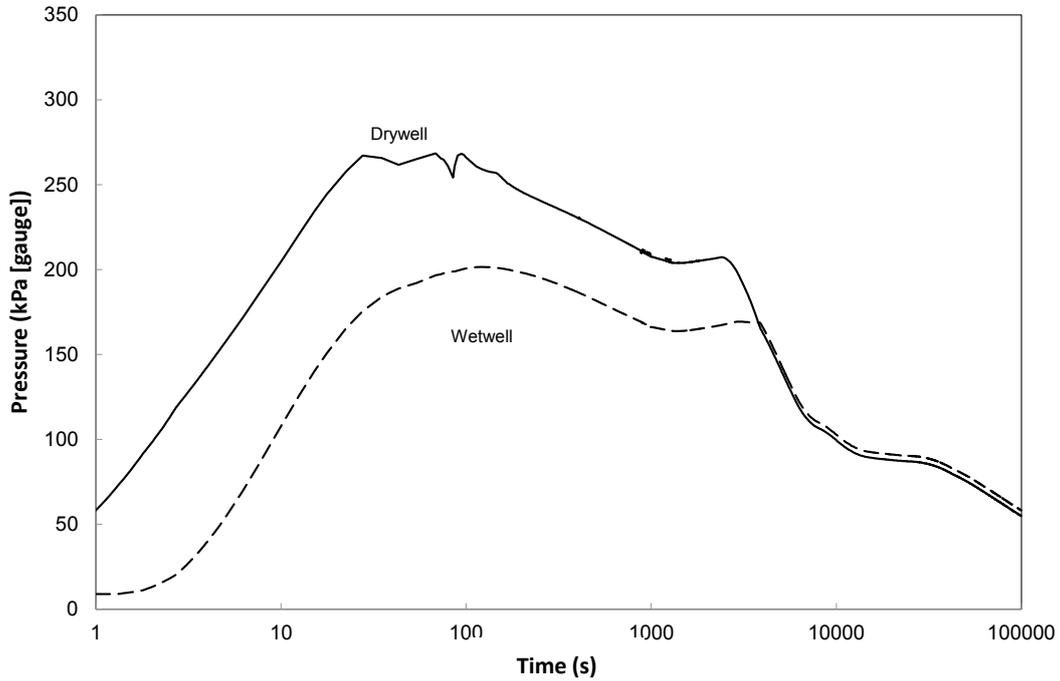


Figure 24.8.3-5: Pressure Transients in the D/W and S/C for Feedwater Line Break Accident (long-term)

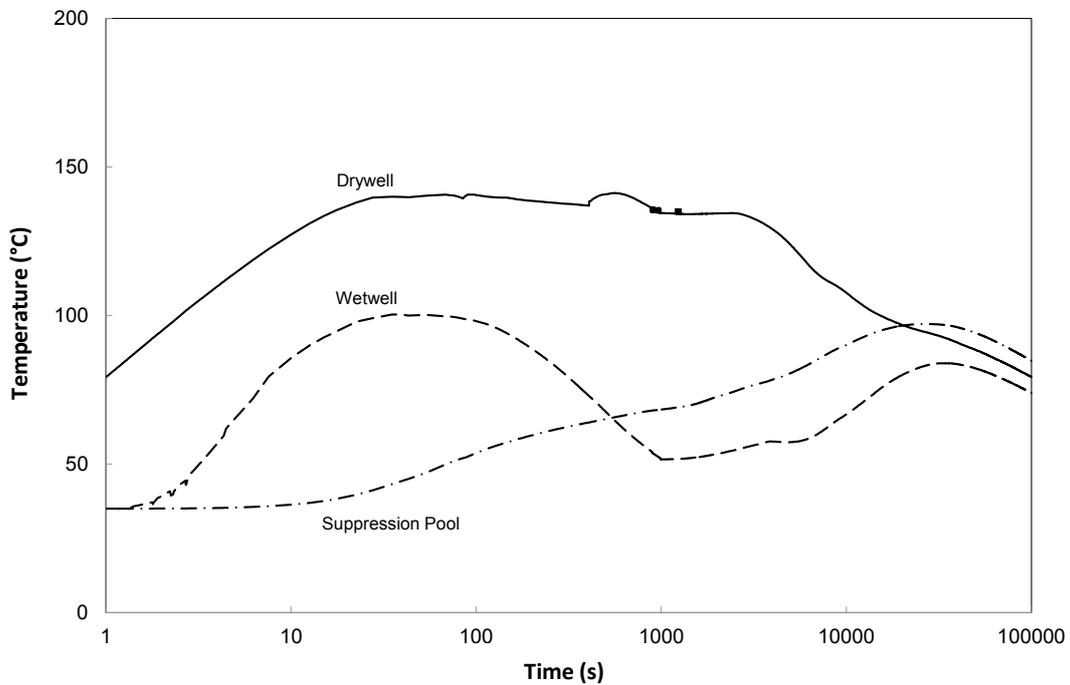


Figure 24.8.3-6: Temperature Transients in the D/W and S/C for Feedwater Line Break Accident (long-term)

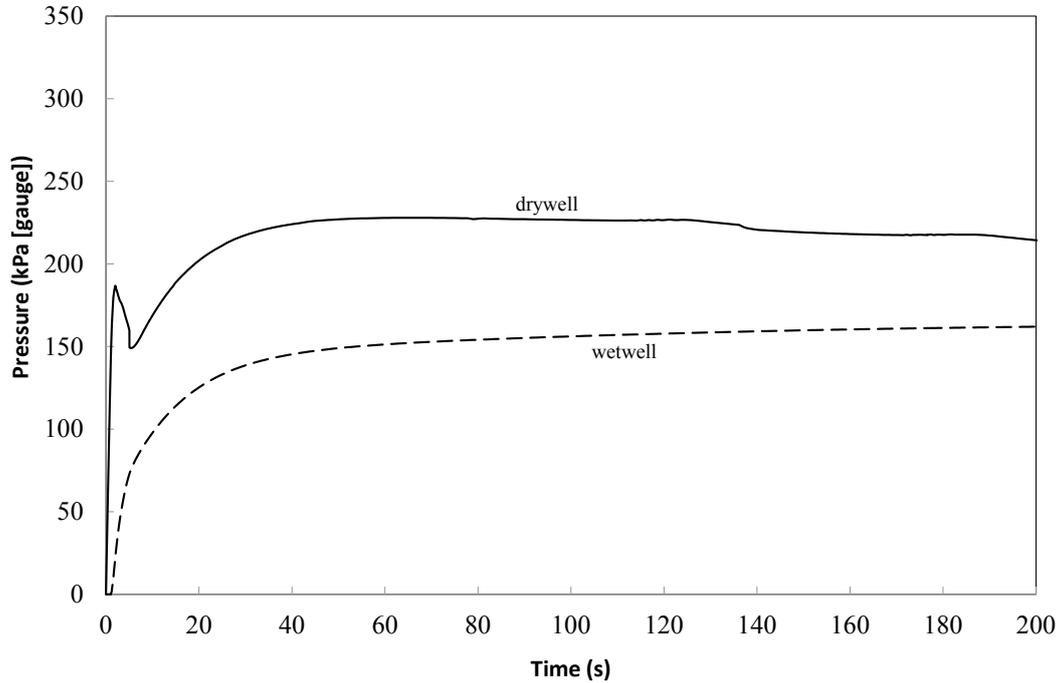


Figure 24.8.3-7: Pressure Transients in the D/W and S/C for Main Steam Line Break Accident (short-term)

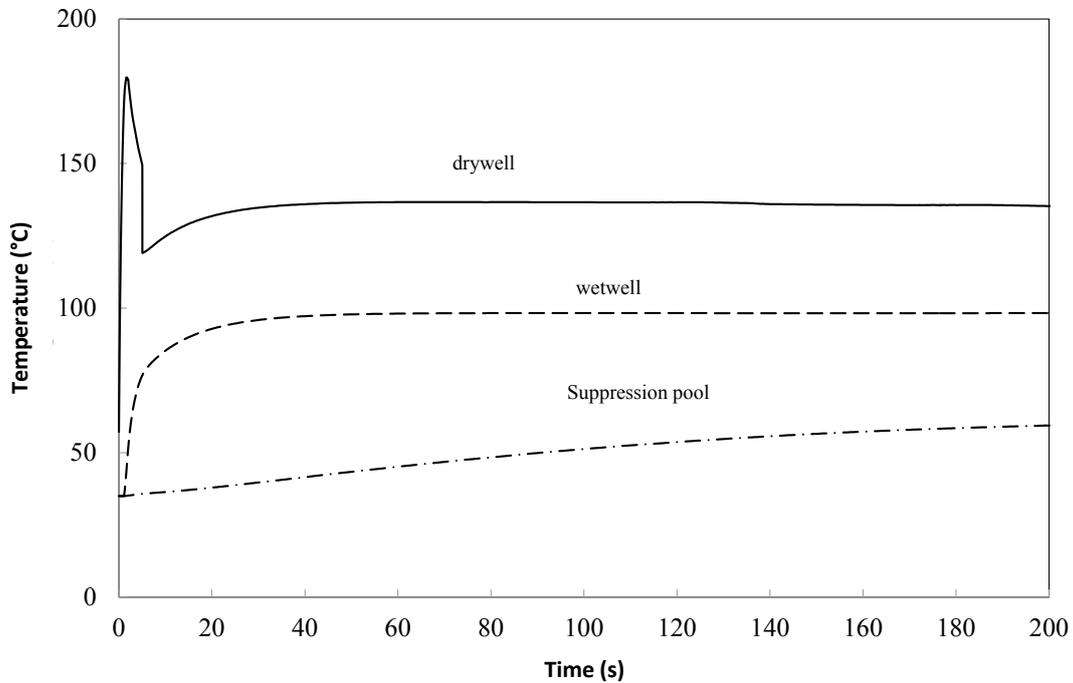


Figure 24.8.3-8: Temperature Transients in the D/W and S/C for Main Steam Line Break Accident (short-term)

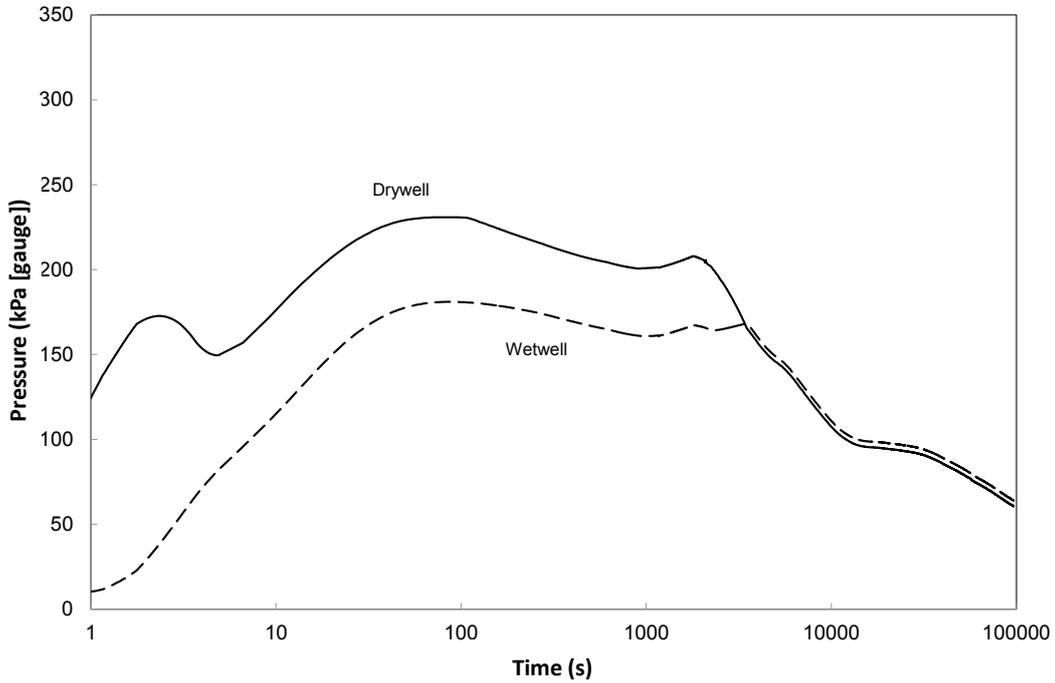


Figure 24.8.3-9: Pressure Transients in the D/W and S/C for Main Steam Line Break Accident (long-term)

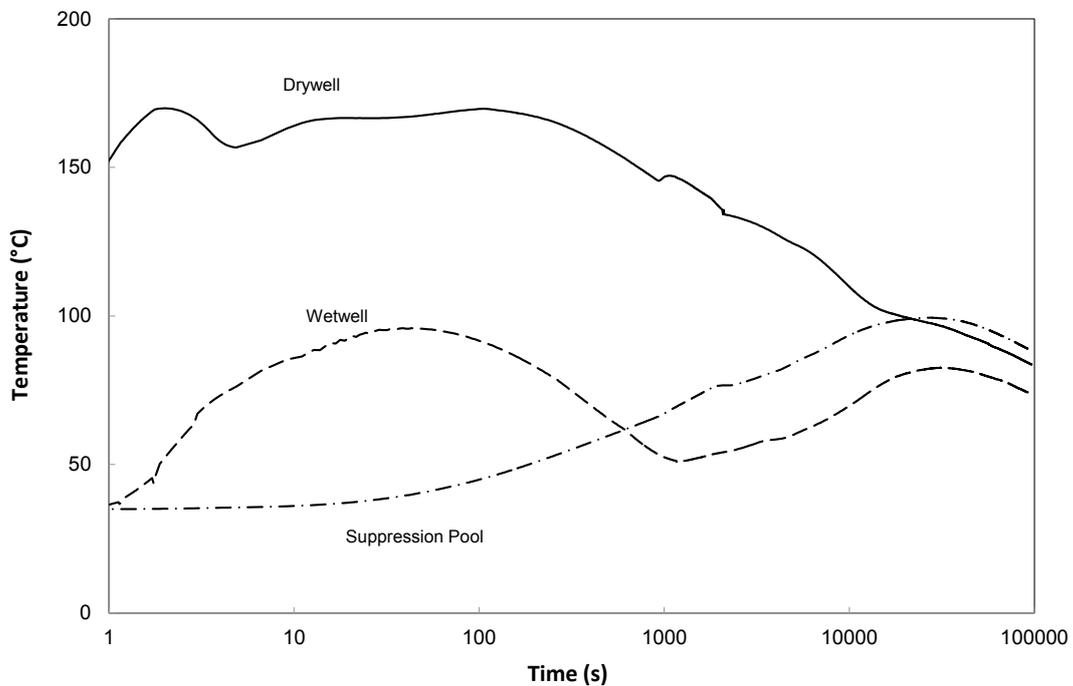


Figure 24.8.3-10 : Temperature Transients in the D/W and S/C for Main Steam Line Break Accident (long-term)

(II) Analysis of Concentration of Flammable Gases in the PCV

Following a design basis LOCA, hydrogen and oxygen are generated by radiolytic decomposition of the water in the reactor core. These are the only significant sources of post-accident hydrogen and oxygen generation since the fuel cladding temperature is too low for a metal-steam reaction to produce hydrogen. If the concentrations of hydrogen and oxygen are not controlled, a flammable gas mixture could be produced. To ensure that a combustible gas mixture does not form, the oxygen concentration is kept below 5 vol%, or the hydrogen concentration is kept below 4 vol%.

The concentration of flammable gases in the PCV following a LOCA may be controlled by the FCS, which consists of Passive Autocatalytic Recombiners (PARs). The PARs are assumed to be located inside of the PCV and to perform automatically actuated by convection flow in the PCV.

(a) Analysis Assumptions

The following assumptions are used in the analysis:

- (i) It is assumed that the reactor had been operating about 102% of the rated power (i.e. at 4005 MW) immediately before the onset of the accident.
- (ii) Since oxygen concentration in the PCV is maintained during normal operation to be 4 vol% or less by the Atmospheric Control System (AC), the initial oxygen concentration in the PCV is assumed to be 4 vol%.
- (iii) Initial humidity is assumed to be 100% relative humidity. This leads to a low initial amount of non-condensable gas (nitrogen).
- (iv) Immediately before the onset of the accident, the D/W temperature is assumed to be 57 °C; the S/P water temperature is assumed to be 35 °C. These temperatures are in normal operating conditions. The pressure inside the containment vessel is assumed to be 5 kPa [gauge].
- (v) Hydrogen generation by metal-water reaction and Fission product (FP) release to the PCV are not considered. According to the results of the ECCS analysis (shown in Section 24.8.2.1), the maximum peak cladding temperature is around 641 °C during the bounding DBA LOCA event. Therefore, the integrity of fuel cladding is expected to be maintained and there is no need to consider any Fission Product (FP) release.
- (vi) The reactor coolant activity inventory is assumed to include FPs from pre-existing pin hole failures of fuel and includes an iodine spike caused by the depressurisation of the coolant allowing additional iodine to be released from the fuel as described in the Source Term definitions in Chapter 20. The fraction of FP radiation energy absorbed by coolant is assumed to be follows:

1) Beta

- Betas from FPs in the fuel rods: 0%

(All betas from the fuel rods are assumed to be absorbed by the fuel cladding).

- Betas from FPs intimately mixed with the coolant: 100%

2) Gamma

- Gammas from FPs in the fuel rods, coolant in the core region: 10%

(Ninety percent of gammas in the fuel rods are assumed to be absorbed by the fuel cladding).

- Gammas from FPs intimately mixed with the coolant, all coolant: 100%

(vii) Hydrogen yield rate (G value) is 0.2 molecule/100 eV and Oxygen yield rate (G value) is 0.1 molecule/100 eV.

(viii) The PARs automatically operate when the hydrogen concentration exceeds 1.5 vol% and the oxygen concentration simultaneously exceeds 2.5 vol%. When the hydrogen concentration falls to below 1.5 vol% or the oxygen concentration falls below 2.5 vol%, recombination stops automatically until starting conditions shown above are met again.

(ix) Four PARs are installed in the D/W and one of them is assumed to be failed. (For the purposes of the assessments performed in GDA, the FCS has been assumed to contain five units of PARs. It has also been assumed 4 units are set in the D/W and 1 unit is set in the Wetwell (W/W)).

(x) One division of ECCS is assumed to be available.

(b) Fault Progression

Following a design basis LOCA, hydrogen and oxygen are generated by radiolytic decomposition of the water in the reactor core. Generated hydrogen and oxygen are released into the drywell through the break. Therefore, concentrations of hydrogen and oxygen in the D/W increase gradually.

When the hydrogen concentration reaches 1.5 vol%, the PARs operate automatically (assuming sufficient oxygen concentration), and if the hydrogen concentration falls to below 1.5 vol%, recombination stops automatically until the hydrogen concentration reaches (exceeds) 1.5 vol% again.

(c) Analysis results

Figure 24.8.3-11 shows the analysis result without PARs operating. Since the PCV atmosphere is inerted with nitrogen prior to the accident, the flammable gas concentration in the PCV does not reach the flammable limit [Ref-30] until 104 hours after the LOCA.

Figure 24.8.3-12 shows the analysis result with PARs. The PARs automatically operate at 26 hours after the LOCA (hydrogen concentration reaches 1.5 vol%). After this, the hydrogen concentration in the PCV is kept from exceeding 1.5 vol%. Therefore, the flammable gas concentration in the PCV does not reach the flammable limit.

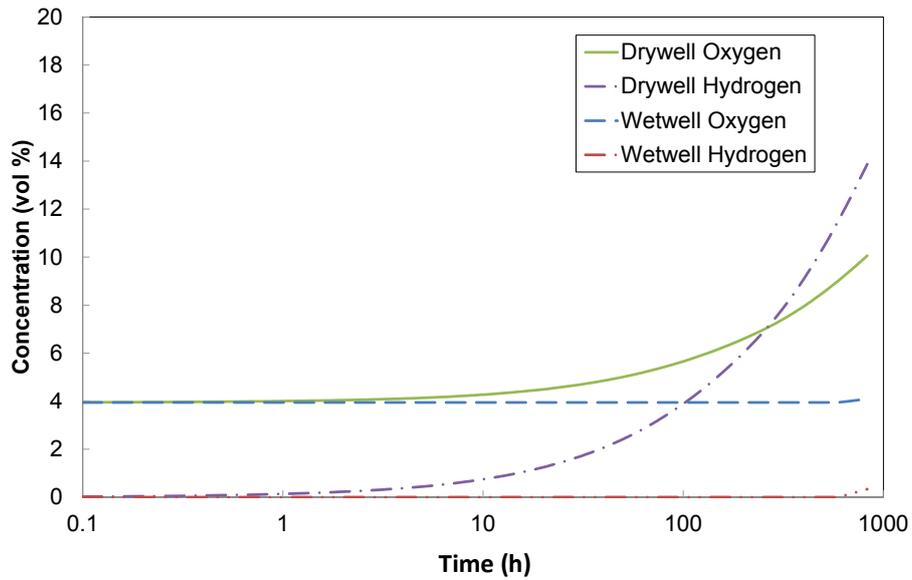


Figure 24.8.3-11: Hydrogen and Oxygen Concentrations in Primary Containment (without PARs)

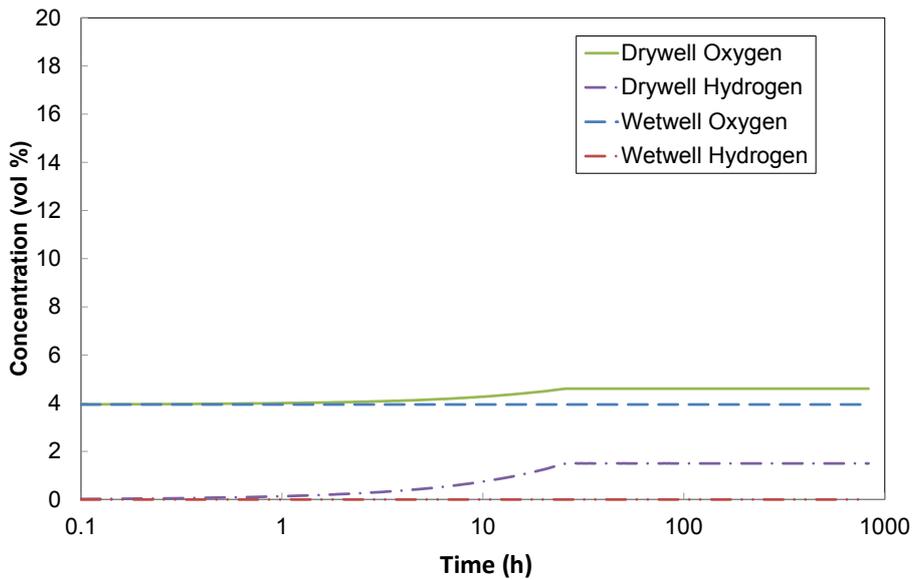


Figure 24.8.3-12: Hydrogen and Oxygen Concentrations in Primary Containment (with PARs)

(III) Dose Evaluation

The evaluation of the radiological consequences of a design basis LOCA includes both off-site dose evaluations and a control room dose evaluation, and the acceptance criteria AC-D5 and AC-D6 apply. The LOCA is assumed to occur following a double ended guillotine rupture of a limiting line, which maximises the potential for fuel damage. As the hydraulic analysis results in Section 24.8.2 show that there is no failure of the fuel following a Design Basis LOCA, additional fission products are not released from the core to the containment. The only Fission Products are from any pre-existing pin hole failures as discussed earlier. The analysis is based upon the process flow diagram shown in Figure 24.8.3-13.

(a) Fission Product Release and Pathway to the Environment

It is assumed that the fission products found in the primary coolant are released into the containment and are available for release to the environment. As an iodine spike is considered based on the UK ABWR source term, the chemical species differentiation for the iodine isotopes released to the containment atmosphere is assumed to be 96.8% elemental form, 3.2% organic form [Ref-17]. Following the release of fission products to the containment atmosphere from the reactor pressure vessel, the fission products are subject to holdup and radioactive decay, removal processes, and leakage to other plant areas and to the environment. Two specific pathways are analysed in releasing fission products to the environment.

(b) Primary Containment Leak

The first pathway considered is leakage to the Reactor Building (secondary containment) via penetrations and engineered safety feature (ESF) components. This leakage is assumed to be 0.4% per day of the primary containment free air volume based on design parameters. In this analysis, the pressure and temperature transient during the accident is considered for evaluation of leakage from the primary containment. The secondary containment is a multi-compartment self-contained structure maintained at negative pressure with respect to the environment, thereby providing a significant holdup volume for fission product releases. All leakage pathways from the primary containment, except the main steamlines, the feedwater lines and the drywell sump discharge lines, terminate in the Reactor Building. Flow through the Reactor Building/secondary containment is directed via the Standby Gas Treatment System (SGTS) to the stack through High Efficiency Particulate Air (HEPA) and charcoal filters. Credit is taken for holdup, assuming 50% mixing in the secondary containment without plateout and other removal processes except filtration in the SGTS.

(c) Main Steamline Modelling

Leakage through the steamlines is modelled as described below, and leakage through the feedwater lines is assumed to be negligible assuming the proper isolation and filling of the feedwater lines upstream of the primary containment through the feedwater system.

The potential release and transport pathway is via the main steamline through leakage in the main steamline isolation valves. It is assumed that a pathway exists, which permits the primary containment atmosphere direct access to the main steamlines and that the MSIVs leak at the maximum technical specification limit as discussed in Chapter 20.

The MSIV leakage depends on containment pressure. The MSIV leakage flows through the MSL and MSL drain lines where deposition of radionuclides on the pipe walls is credited.

(d) Plateout, Surface Fixation, and Resuspension

Gaseous iodine is known to deposit on surfaces (plateout) and undergo physical and chemical changes to be re-emitted as an airborne gas (resuspension) or become permanently fixed to the surface (fixation). Evaluation of these phenomena is an important component of accident condition analyses such as LOCA dose analysis.

(i) Plate-Out

1) Piping Decontamination Factors

The decontamination factors (DFs) are based on the Cline model for deposition velocities. Note that plateout of organic iodine is neglected (DF = 1).

2) Piping Plate-Out Determination

The deposition velocities for particulate and elemental iodine are considered. Deposition of elemental iodine is based on the Cline model, and deposition of particulate (aerosol) iodine is based on the Brockmann-Bixler model. The Cline model is more conservative for removal of elemental iodine resulting in less iodine plateout, and more activity transported to the condenser.

3) Condenser

As turbine main condenser is not safety grade, the plate out and decay over the transfer time in pipe after the MS bypass valve and in main condenser are not credited.

(ii) Re-suspension

1) Surface Fixation

Surface fixation is based on the assumption that the fixation rate increases with temperature. The surface fixation rate is a required factor in the resuspension rate formula. The fixation rate used in this analysis is based on the Cline model.

2) Resuspension Rate Determination

Once iodine plates-out on the surface of a pipe, it has the potential to become re-suspended and

once again become available for release to the environment. The Cline model presents formulas for resuspension of iodine. The resuspension rate varies for each chemical form of iodine. Note that once the iodine is re-emitted it is assumed to instantaneously transport to the condenser and be available for release to the environment. Only plateout of elemental and particulate iodine is considered, and all re-suspended iodine is assumed to be organic iodine.

(e) Key parameters

The key parameters for accident analysis are specified as follows:

(i) Standby Gas Treatment System Parameters

SGTS flow rates:

- 0 - 30 minutes: 100%/day (2 SGTS)
- > 30 minutes: 50%/day (1 SGTS)

Filter efficiency:

- 0 - 30 minutes: 99.9%
- > 30 minutes: 99.9% (all iodine species)

(f) Analysis Results

As there is no FP release from the fuel during a Design Basis LOCA and FP concentration in the primary coolant is low, if a LOCA occurs, only a small amount of FP is expected to be released into the primary containment. Furthermore the containment is leak-tight and the FPs pass through a filtered system (SGTS). Hence the amount of FP released to the environment is very small, if not insignificant. As a result of the dose evaluation, off-site and on-site consequences are demonstrated to be much lower than the AC-D6 and AC-D5 acceptance criteria, and lower than the BSO as shown in Table 24.8-7.

Table 24.8-7: Doses to exposed persons from LOCA-Feedwater Line Break- event (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	2.1E-04	8.2E-05	5.7E-05	AC-D6 (BSL): 1.0E+02 BSO: 1.0E-02
On-site (Control Room)	N/A	N/A	5.9E-06	AC-D5 (BSL): 5.0E+02 BSO: 1.0E-01

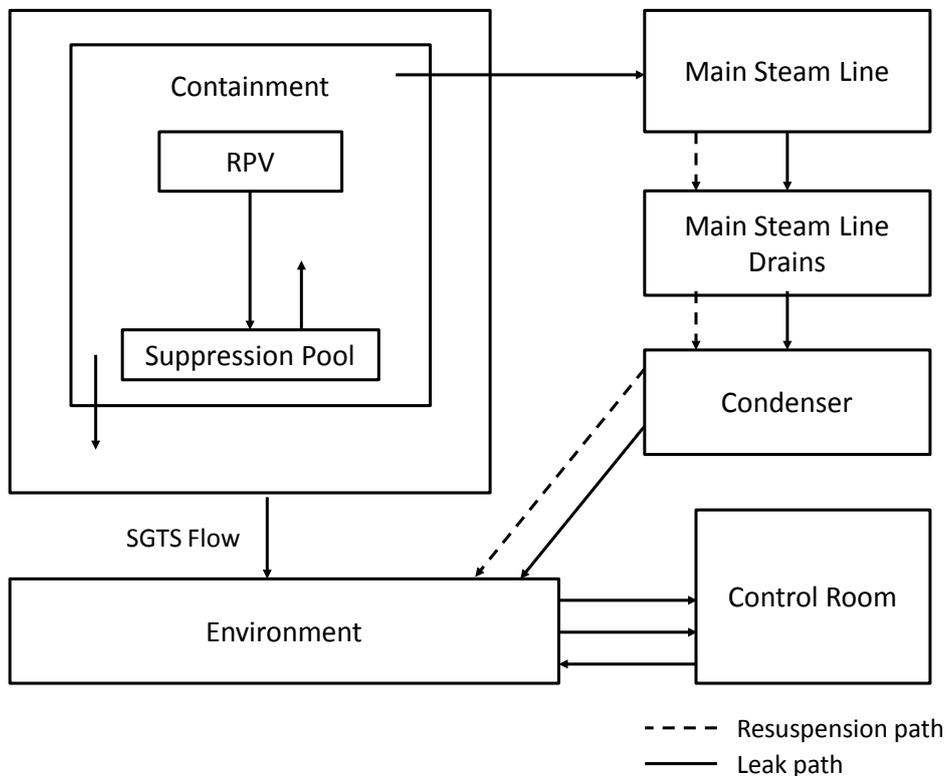


Figure 24.8.3-13: LOCA inside Primary Containment Release to Environment

(4) Discussion and Conclusions

As a result of evaluation of the PCV performance, it has been verified that the Acceptance Criteria related to containment are satisfied for the accidents being analysed.

As a result of the dose evaluation, off-site and on-site consequences have been demonstrated to be much lower than the AC-D6 and AC-D5 acceptance criteria, and lower than the BSO. This is due to the fact that there is no fuel failure in these events and the dose rate from LOCAs is limited to doses from the activity contained in the coolant at the beginning of the event.

In addition, as a result of evaluation of the concentration of flammable gases, it has been verified that the concentrations of flammable gases are kept lower than the combustion limit values of hydrogen (4 vol%) and oxygen (5 vol%).

The results of the analysis of this fault show that all the acceptance criteria are met and those relating to fuel failure and public and worker dose are met with a large margin. In addition, only Class 1 protection is claimed in the analysis, whereas there are additional Class 2 SSCs (FLSS, etc.) that can protect against the fault should the Class 1 SSCs not be available. The margin on acceptance criteria

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

and the availability of additional protection make the risk from this fault very low. There are no additional reasonably practicable means of further reducing the risk and the risk is deemed to be ALARP.

NOT PROTECTIVELY MARKED

24.8.4 LOCA outside Primary Containmentment

This is similar to the LOCA event described in the previous section except that the break occurs outside of the primary containment.

The following cases are in the LOCA outside primary containment fault group:

- Main steam line break outside primary containment – see Section 24.8.4.1
- Reactor Water Clean-up line break outside primary containment
- Feedwater line break outside primary containment
- Small line break outside primary containment – see Section 24.8.4.2

The main steam line break outside primary containment is the bounding fault that is analysed as described below. This is an infrequent fault. For a feedwater break outside primary containment, the check valves in the feedwater line prevent the release of water outside the primary containment.

Protection against this fault is provided by the ECCS as for other LOCAs and as listed in Table 24.8-1. In addition, isolation of the reactor coolant circuit is provided by the MSIVs to limit the release of radio activity to the environment. In any case, flow through the MSIVs are limited by flow restrictors.

Analysis conditions are as for other LOCAs and are listed in Table 24.8-4.

24.8.4.1 Main Steam Line Break outside Primary Containment

Fault Schedule Ref: 10.1

(1) Description of Fault

For this fault, it is assumed that the Main steam line fails outside the primary containment, leading to reactor coolant being discharged outside the primary containment, potentially to the environment via the Turbine Building.

The event bounds

- Reactor Water Clean-up line break outside primary containment (Fault Schedule Ref: 10.2)
- Feedwater line break outside primary containment (Fault Schedule Ref: 10.3)

(2) Plant Normal Response

The normal plant response is to automatically scram the reactor and initiate ECCS as in the fault assessment.

(3) Analysis of Event

The analysis of this event is presented in three parts:

- ECCS Analysis (Single Failure Assumption)
- ECCS Analysis (Combination of Maintenance Unavailability and Single Failure)
- Dose Evaluation

(I) ECCS Analysis (Single Failure Assumption)**(a) Analysis Assumptions**

The analysis conditions are chosen to be conservative and are as follows:

- (i) Analysis conditions are as shown in Table 24.8-4.
- (ii) A conservative value of the gap conductance between the fuel clad and pellet is used in the consideration of changes during the exposure (fuel burnup) cycle.
- (iii) Instant double-ended break of one of the four main steam lines outside primary containment is assumed. Frictional losses between the RPV and the break are not considered in the evaluation of the amount of discharged coolant.
- (iv) The main steam isolation valves are assumed to be completely closed 5 seconds after the

accident (including 0.5 seconds valve actuation delay time) on a high flow rate signal in the main steam line.

- (v) Reactor scram is assumed to be initiated concurrently with the occurrence of the fault.
- (vi) The release flow rate is assumed to be restricted to 200% of rated flow rate by the MSL flow restrictors until the flow rate is restricted by the main steam isolation valve.
- (vii) The Moody model is used as the critical flow model for calculation of the break flow rate.
- (viii) Off-site power is assumed to be lost concurrently with the occurrence of the accident and consequently, all 10 RIPs are assumed to trip instantaneously.
- (ix) The most conservative single failure is assumed in the ECCS network from the viewpoint of its impact on the reactor cooling capability. The most conservative single failure in the case of the main steam line break outside primary containment is a failure of an emergency diesel generator that supplies power to an HPCF division.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

AC-D5: Dose to workers should be less than 500 mSv.

AC-D6: Dose to members of the public should be less than 100 mSv.

(c) Fault Progression

Following the postulated break of a main steam line outside the primary containment, the fault progresses as follows:

- (i) Instantaneous double-ended break of MSL piping, and reactor scram
- (ii) Decrease in RPV pressure, inventory and core flow rate (Blowdown phase)
- (iii) Start of MSIV closure
- (iv) Start of steam and water discharge
- (v) Completion of MSIV closure
- (vi) Start of coolant injection by the RCIC on low reactor water level (Level 1.5)
- (vii) Start of coolant injection by the HPCF on low reactor water level (Level 1.5)

(viii) Recovery of water level inside the core shroud

During the blowdown phase, heat transfer from the fuel to the coolant undergoes a boiling transition from nucleate boiling (normal conditions) to film boiling. The core remains covered throughout the fault progression.

(d) Analysis Results**(i) Mass leaving the RPV through the steam line break**

Steam from the broken pipe is discharged directly from the upstream broken end of the pipe. At the same time, steam from the other three intact pipes backflows to the break location through the main steam header upstream of the turbine stop valve and is discharged from the pipe break.

The amount of steam discharged from the broken area increases from about 102% of the rated flow rate before the accident to a rate corresponding to critical flow at a main steam nozzle. Because this value exceeds the rate of steam generated at the core, reactor pressure is reduced. The void fraction in the reactor increases due to this decrease in reactor pressure, and the reactor water level increases, reaching the main steam nozzle in about 2 seconds. After that, steam and water are discharged from the broken area.

The main steam isolation valves are completely closed in 5 seconds (including a 0.5 seconds valve actuation delay time) after the accident on a high flow rate signal in the main steam pipe. Figure 24.8.4-1 shows mass flow leaving the RPV through the steamline break and Figure 24.8.4-2 shows reactor pressure.

The total integrated mass leaving the RPV through the steamline break until the MSIVs are completely closed are as follows:

Steam: approximately 1.3×10^4 kg

Water: approximately 1.5×10^4 kg

(ii) Responses of fuel cladding temperature, and perforation and oxidation of fuel cladding

Because off-site power is assumed to be lost simultaneously with the accident, core flow rapidly decreases because of trip of the recirculation pumps.

Due to the rapid decrease of core flow, MCPR decreases below the Safety Limit MCPR value at about 1 second after the accident and boiling transition occurs as far as the fourth spacer position from the top of the fuel assembly. Consequently, the heat transfer coefficient from the fuel cladding decreases and the fuel cladding temperature increases. However, the increase of fuel cladding temperature stops after a short time because of the decrease of power due to

reactor scram.

On the other hand, the water level inside the core shroud starts to decrease. However, the RCIC is activated by the low reactor water level (Level 1.5) signal and starts water injection at about 236 seconds after the accident. The HPCF is also activated by the low reactor water level (Level 1.5) signal and starts water injection at about 243 seconds after the accident. The water level inside the core shroud does not decrease below the top of the active fuel, and the core is kept flooded. Therefore, temperature increase of the fuel cladding is limited because the core does not become uncovered. The peak fuel cladding temperature occurs during the boiling transition immediately after the accident.

Figure 24.8.4-3 shows the reactor water level transient and Figure 24.8.4-4 shows the reactor pressure transient during accident. Figure 24.8.4-5 shows the heat transfer coefficient transient at the position of maximum fuel cladding temperature, and Figure 24.8.4-6 shows the fuel cladding temperature transient. The peak fuel cladding temperature during the accident is about 643 °C.

No fuel cladding is perforated during the transient because the hoop stress remains low because the pressure in the RPV remains higher than the internal cladding pressure.

The increase of the oxide layer thickness on the fuel cladding is very small because the fuel cladding temperature is low.

(II) ECCS Analysis (Combination of Maintenance Unavailability and Single Failure)

(a) Analysis Assumptions

The worst case assumption for the MSLB outside primary containment is the unavailability and single failure of the EDGs providing power to the two HPCF divisions.

The other conditions are the same as those shown in item (a) of subsection (I) above, except for (ix).

(b) Fault Progression

Fault progression is the same as shown in item (c) of subsection (I) above, except for (vii).

(c) Analysis Results

The reactor water level slightly decreases compared to the case with only single failure assumption because there is no HPCF injection in this case. The RCIC is activated by the low reactor water level (Level 1.5) signal and starts water injection at about 236 seconds. The water level inside the core shroud does not decrease below the top of the active fuel, and the core is kept flooded. Therefore, temperature increase of the fuel cladding is limited as before because core uncovering does not occur.

The peak fuel cladding temperature occurs during the boiling transition immediately after the accident. The peak cladding temperature is around 643 °C and so the cladding temperature remains much lower than the criterion of 1200 °C to meet the acceptance criterion. (AC-F5 met with significant margin)

Figure 24.8.4-7 shows the reactor water level transient and Figure 24.8.4-8 shows the reactor pressure transient during the accident. Figure 24.8.4-9 shows the fuel cladding temperature transient.

The increase in cladding oxide layer is very small because fuel cladding temperature is relatively low, and it is much less than the 15% limit of the acceptance criterion. (AC-F4 met with significant margin)

The peak cladding temperature and the peak hoop stress are less than the criteria of perforation of fuel cladding. Therefore there is no fuel rupture.

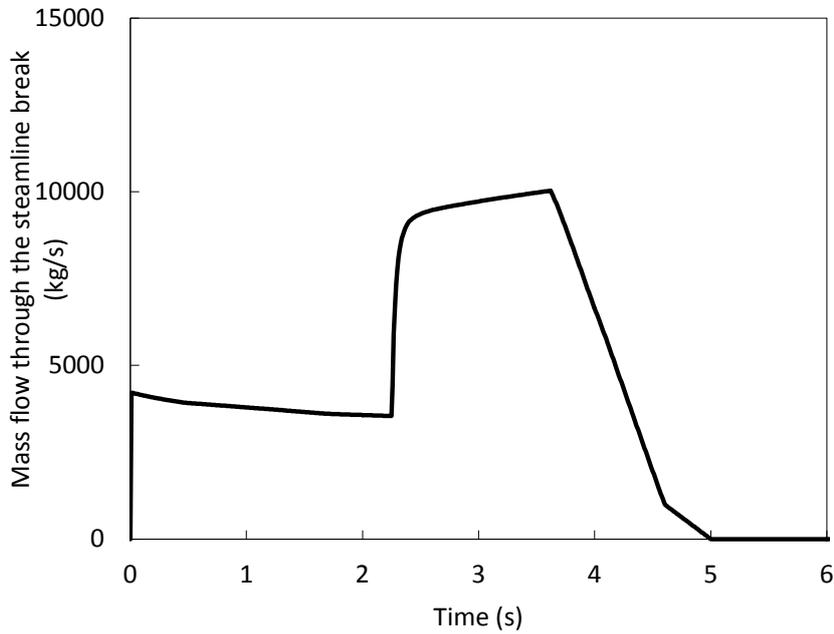


Figure 24.8.4-1: Mass Flow Leaving the RPV through the Steamline Break during Main Steam Line Break outside the Primary Containment

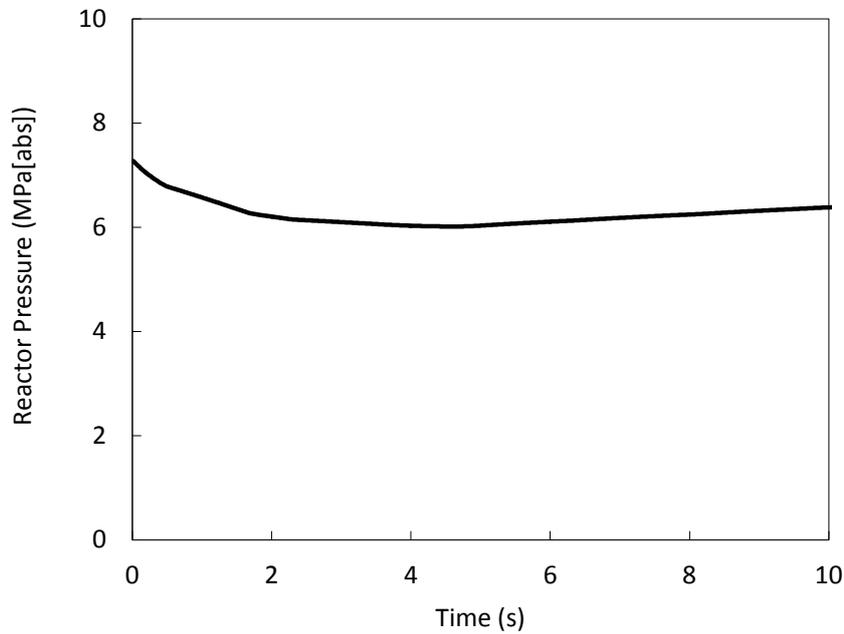


Figure 24.8.4-2: Reactor Pressure during Main Steam Line Break outside the Primary Containment

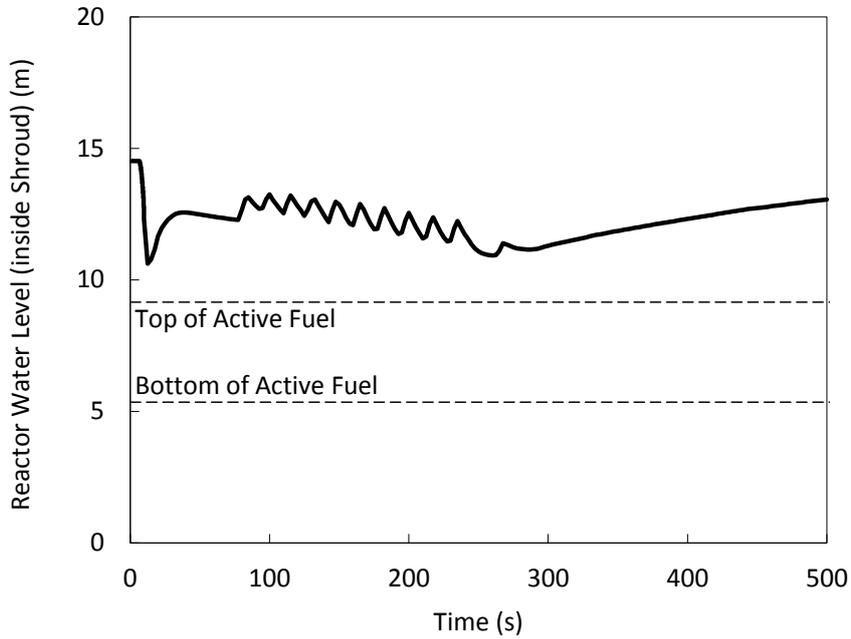


Figure 24.8.4-3: Reactor Water Level during Main Steam Line Break outside the Primary Containment (with RCIC and HPCF)

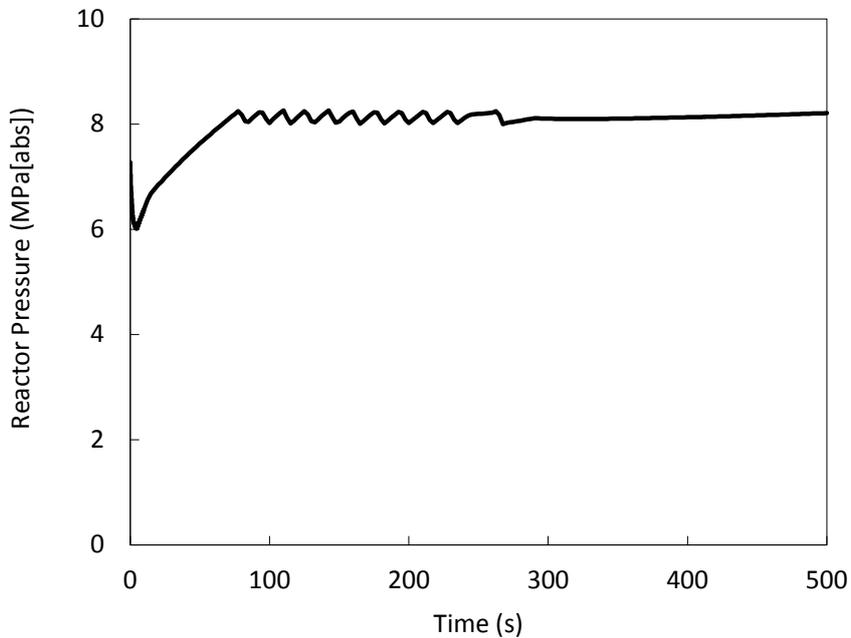


Figure 24.8.4-4: Reactor Pressure during Main Steam Line Break outside the Primary Containment (with RCIC and HPCF)

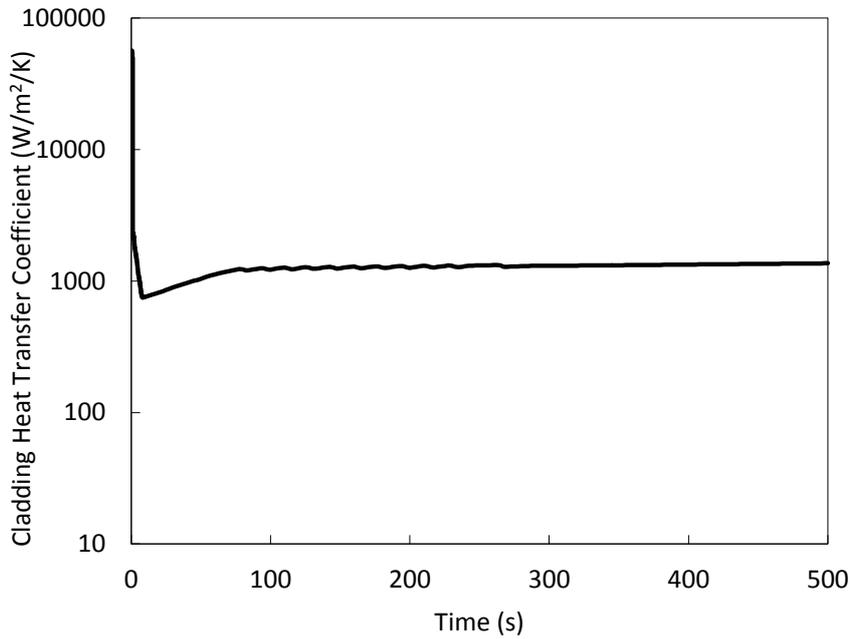


Figure 24.8.4-5: Heat Transfer Coefficient at the Maximum Fuel Cladding Temperature Position during Main Steam Line Break outside the Primary Containment (with RCIC and HPCF)

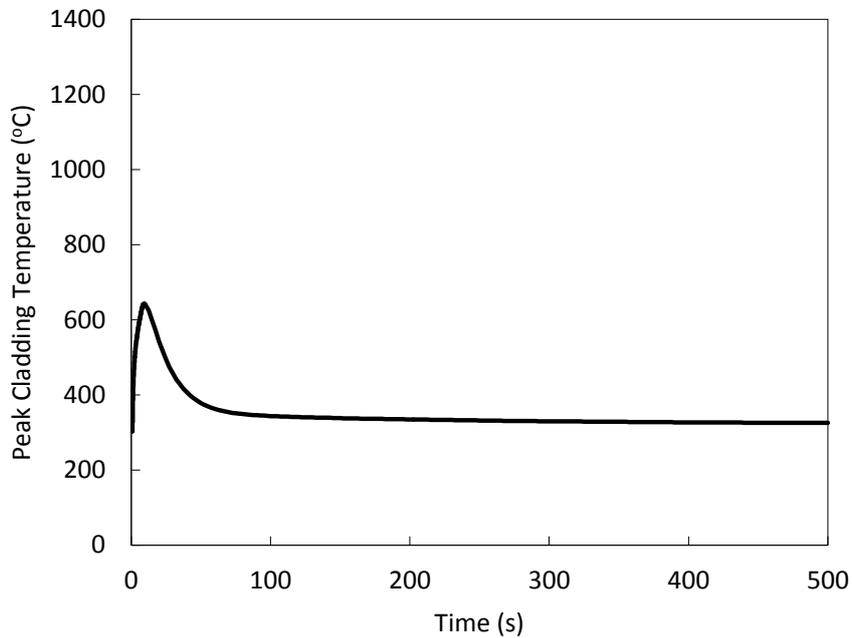


Figure 24.8.4-6: Peak Cladding Temperature during Main Steam Line Break outside the Primary Containment (with RCIC and HPCF)

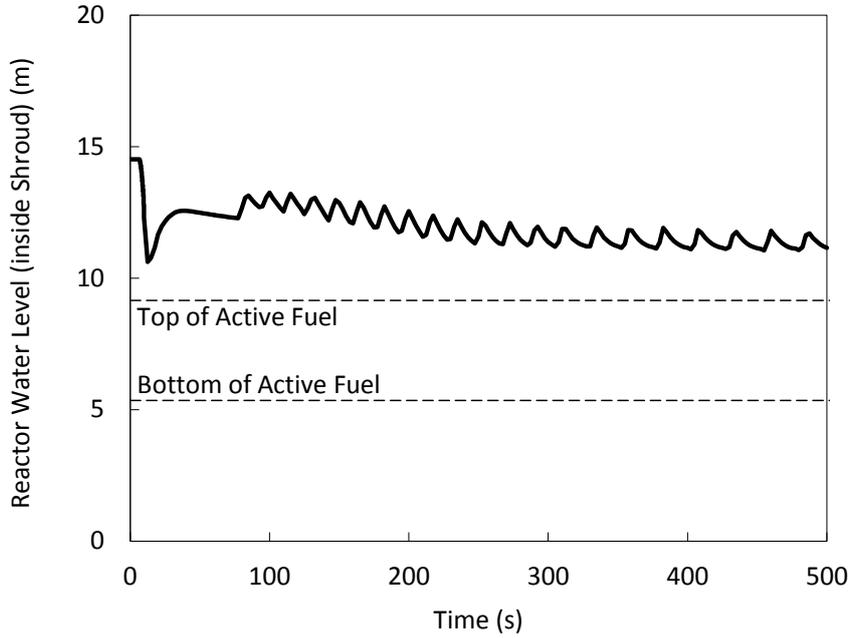


Figure 24.8.4-7: Reactor Water Level during Main Steam Line Break outside the Primary Containment (with RCIC)

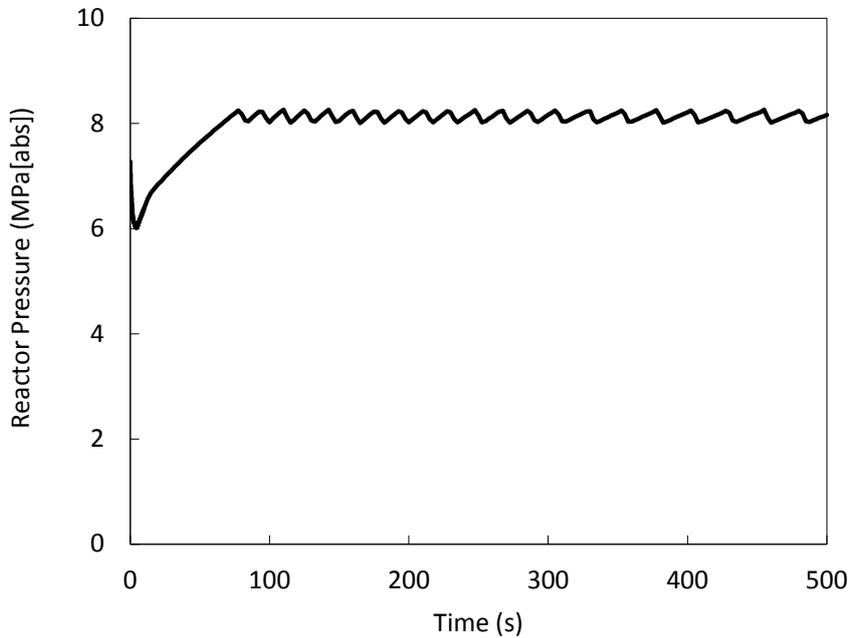


Figure 24.8.4-8: Reactor Pressure during Main Steam Line Break outside the Primary Containment (with RCIC)

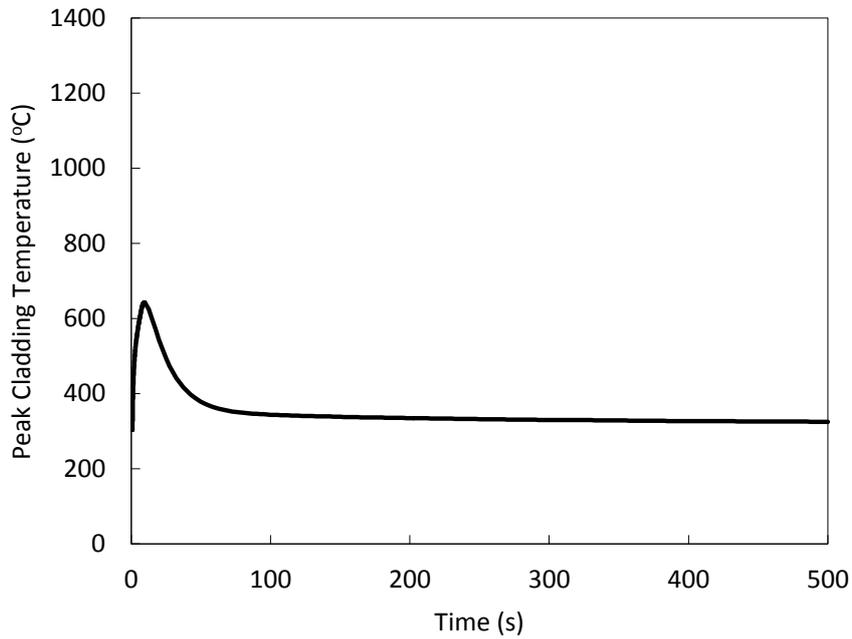


Figure 24.8.4-9: Peak Cladding Temperature during Main Steam Line Break outside the Primary Containment (with RCIC)

(III) Dose Evaluation

The evaluation of the radiological consequences of a design basis MSLB event includes both off-site and on-site dose evaluations and the acceptance criteria AC-D5 and AC-D6 apply for this infrequent fault.

The analysis is based upon a process flow diagram shown in Figure 24.8.4-10.

(a) Fission Product Release and Pathway to the Environment

The MSLB is postulated as a double-ended guillotine brake of MSL outside of the primary containment. It has been demonstrated that there is no fuel damage anticipated during the event. Any dissolved noble gases are assumed to enter the steam phase instantaneously. The mass release from a MSLB is calculated to be 1.5×10^4 kg water and 1.3×10^4 kg steam. The total mass of coolant released is assumed to be the amount in the steam line and connecting lines at the time of the break plus the amount that passes through the valves prior to their closure. For the design basis dose analysis a source term consisting of only the iodine and noble gas is considered. As iodine spike is considered during the accident based on the UK ABWR Source Term (Chapter 20). The total activity release from the MSL to the Turbine Building (T/B) is calculated using the following equation.

Total activity in T/B = (steam mass) \times (steam activity concentration) + (water mass) \times (water activity concentration).

(b) Turbine Building Leak

The pathway is leakage to the environment via the MSL. The entire radionuclide inventory in the T/B is assumed to be released to the environment instantaneously as a ground level release.

(c) Analysis Results

The MSLB outside primary containment is the bounding case for release for Design Basis LOCAs because the containment is bypassed. Public and worker dose is limited by the amount of activity contained in the reactor coolant at the time of the event as there is no fuel failure caused by the event itself. The dose evaluation demonstrates that off-site and on-site consequences are much lower than the acceptance criteria, as shown in Table 24.8-8.

Table 24.8-8: Doses to Exposed Persons from the MSLB outside containment event (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	1.8E-01	6.3E-02	3.8E-02	AC-D6 (BSL): 1.0E+02 BSO: 1.0E-02
On-site (Control Room)	N/A	N/A	2.5E-03	AC-D5 (BSL): 5.0E+02 BSO: 1.0E-01
On-site (T/B operational floor)	N/A	N/A	5.3E-01	AC-D5 (BSL): 5.0E+02 BSO: 1.0E-01

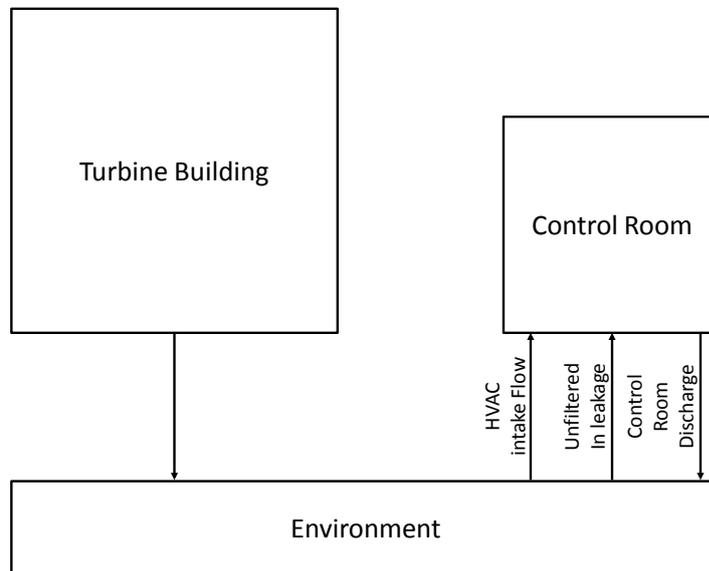


Figure 24.8.4-10: Main Steam Line Break Accident Release to Environment

(4) Discussion and Conclusions

The peak cladding temperature for the MSLB outside primary containment is less than 1200 °C, and the increase in cladding oxide layer is much less than the 15% acceptance criterion value. Thus fuel cladding is not threatened either in terms of peak temperature or oxidation. Therefore there is no fuel damage and any release of fission products inside the fuel cladding is limited. In addition, integrity of the primary containment is not threatened for this event as the piping break occurs outside of the primary containment.

Furthermore, as a result of dose evaluations, off-site and on-site dose consequences are lower than the AC-D6 and AC-D5 criteria values.

The results of the analysis of this fault show that all the acceptance criteria are met and those relating to fuel failure are met with a large margin. In addition, only Class 1 protection is claimed in the analysis, whereas there are additional Class 2 SSCs (FLSS, etc.) that can protect against the fault should the Class 1 SSCs not be available. The margin on acceptance criteria and the availability of additional protection make the risk from this fault very low. There are no additional reasonably practicable means of further reducing the risk and the risk is deemed to be ALARP.

24.8.4.2 Small LOCA outside Primary Containment

Fault Schedule Ref: 10.4

(1) Description of Fault

There are a number of small lines connected to the reactor pressure boundary, which form part of instrumentation systems. The Small Line Break outside the primary containment is the bounding event in terms of frequency of the occurrence, and is designated as a frequent fault.

The Small Line Break is postulated as a small steam or liquid line pipe break outside the primary containment but within the Reactor Building (R/B). The instrument line from the RPV to outside of containment has a 1/4 inch orifice to limit flow at a line break. It also has an excess flow check valve to shut the line on excess flow and a manually operated stop valve. If the instrument line breaks, the operator recognises the break by the instrument error signal. However, the atmospheric condition in the vicinity of the leak continues to deteriorate until the stop valve is closed if a single failure of the excess flow check valve is assumed. In the analysis, it is assumed that the broken line cannot be isolated and reactor coolant continues to release until the primary system is depressurised by the operator.

The fault develops very slowly and the operator scrams the reactor after 30 minutes. In this case, since the release rate from the small line is very low, reactor water level is controlled by the water level control system. Therefore, no fuel damage is expected for this event. However, the operator also has the option to manually actuate the ECCS or the FLSS to provide makeup water.

(2) Plant normal response

If the fault occurred, the leak may result in noticeable increases in radiation, temperature, humidity, or noise levels in the R/B or abnormal indications of actuations caused by the affected instrument. The operator can use a large number of process indications to identify the break and isolate it. The operator action is initiated with the discovery of the unisolable leak. The action consists of the orderly shutdown and depressurisation of the reactor vessel.

(3) Analysis of Event**(a) Analysis Assumptions**

Table 1 of the Topic Report on Design Basis Analysis [Ref-5] attachment F shows the core power, compartment volumes, iodine chemical fractions, SGTS parameters for buildings, and occupancy factors used in the Small Line Break dose analysis. The following details the assumptions used for the Small Line Break dose analysis which are not listed in Table 1 of Topic Report on Design Basis Analysis [Ref-5] attachment F.

Figure 24.8.4-11 shows the release and transport pathway to the environment of the Small Line Break outside primary containment.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

AC-D1: Dose to workers should be less than 20 mSv.

AC-D2: Dose to members of the public should be less than 1 mSv.

(c) Fault Progression

Reactor coolant is released into the R/B through the instrument line for 30 minutes at normal operating temperature and pressure. It is assumed that the operator scrams the reactor to depressurise the reactor at 30 minutes.

The flow through the small instrument line is limited by the 6mm diameter orifice.

The operator brings the reactor to a cold shutdown state. The total released coolant mass until cold shutdown conditions are achieved is calculated.

(d) Analysis Results

The concentration of nuclides in the reactor coolant for the Small Line Break analysis is based on the source term [Ref-18]. Spike release from fuel due to depressurisation of the core is considered. The amount of the spike source term is assumed to be based on the pressure ratio between the normal operation pressure and accidental pressure at each time step.

As described above, operator action is expected after 30 minutes. The reactor coolant flows into the R/B at the maximum rate until 30 minutes. The reactor is depressurised by a normal shutdown operation at 30 minutes, and reactor coolant flow decreases corresponding to the decreasing reactor pressure. Since iodine spike is proportional to the depressurisation ratio, the radioactivity concentration caused by an iodine spike increases corresponding to reactor pressure. It is assumed that the break flash fraction is 0.38 in the analysis. The retention effect in the building is assumed to be $DF = 10$ for nuclides other than noble gas and iodine. The R/B ventilation system isolates 30 minutes after occurrence of the event. The contamination is processed by the SGTS and subsequently released to the environment. The SGTS is credited for the event with a filter efficiency of 99.9% for all iodine chemical species. As a result of the dose evaluation, off-site and on-site consequences are demonstrated to be much lower than the BSL and the BSO values as shown in Table 24.9-8.

Table 24.8-9: Doses to Exposed Persons from a Small Line Break (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	1.3E-04	6.7E-05	5.2E-05	AC-D2 (BSL): 1.0E+00 BSO: 1.0E-02
On-site (Control Room)	N/A	N/A	8.9E-06	AC-D1 (BSL): 2.0E+01 BSO: 1.0E-01

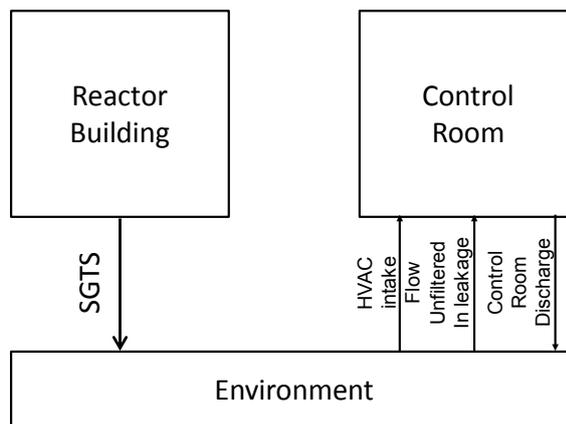


Figure 24.8.4-11: Small Line Break Release pathway to the Environment

(4) Discussion and Conclusions

Off-site and on-site consequences are much lower than AC-D2 and AC-D1 and the BSO values as shown in Table 24.9-8. Therefore, the acceptance criteria described above are demonstrated to be met for this event.

The results of the analysis of this fault show that all the acceptance criteria are met and those relating to fuel failure and public and worker dose are met with a large margin. In addition, only Class 1 protection is claimed in the analysis, whereas there are additional Class 2 SSCs (FLSS, etc.) that can protect against the fault should the Class 1 SSCs not be available. The margin on acceptance criteria and the availability of additional protection make the risk from this fault very low. There are no

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

additional reasonably practicable means of further reducing the risk and the risk is deemed to be ALARP.

NOT PROTECTIVELY MARKED

24.9 Analysis Results and Fault-based View – Common Cause and Multiple Failures

This section gives analyses for events resulting from common cause or multiple failures, including those where the Class 1 provision of HLSFs fail due to Common Cause Failure (CCF). The section covers three main types of event:

- Anticipated Transients without Scram – see Section 24.9.1
- Station Blackout – see Section 24.9.2
- Events caused by CCF of essential support systems – see Section 24.9.3

24.9.1 Anticipated Transient without Scram (ATWS)

An Anticipated Transient without Scram (ATWS) is a particular case of a frequent fault with failure of Class 1 protection in that an ATWS event can be any of the transients listed in Table 24.4-1 plus failure of the HLSF 1-3 Emergency Shutdown of the Reactor. This failure comes about through failure of the Class 1 scram function provided by the CRDs supported by SSLC (RPS) (see Table 24.6-1) in any part of that system including sensors or detectors, logic, actuation or the control rods themselves. ATWS is categorised as an infrequent design basis fault for the UK ABWR.

Hitachi-GE's NSEDPs [Ref-24] require that for all frequent design basis faults there should be diverse provision of all HLSFs and that this provision should be at least Class 2. This principle applies to ATWS as it is a frequent design basis fault with loss of HLSF 1-3. Therefore, the design provides diverse Class 2 scram functions (HLSF 1-5 Functions of alternative reactivity control) as shown in Table 24.9-1 and Figure 24.9.1-1.

Firstly, HWBS tries to insert the control rods using ARI and core flow is reduced to reduce the core reactivity by tripping the RIPs (ATWS-RPT) and feedwater stop (FWSTP). If the control rods fail to insert, after 3 minutes, HWBS actuates boron injection using SLC. The set points and other parameters associated with these systems are shown in Table 24.9-2.

The ATWS response is normally automatic. However, it is also possible for the operator to initiate scram manually. The corresponding HBSCs are: HF ARI 1-5.1 and HF SLC 1-5.1. There is also a HBSC where the operator recognises the need to scram the reactor manually in advance of an ATWS event: HF CRD 1-3.1.

The representative ATWS event is Main Steam Isolation Valve Closure with failure to scram. The analysis of this event is presented in 24.9.1.1 to show the effectiveness of the ATWS protection described above and in Table 24.9-1. In the analyses SLC is credited to achieve reactor hot shutdown, rather than ARI, because SLC takes longer time to achieve hot shutdown than ARI and this results in the containment pressure and the suppression pool temperature being more severe. Therefore the ARI cases are bounded by SLC cases and are not analysed. Further detail and assessment of some other ATWS events are described in the Topic Report on DBA [Ref-5].

During the 1980s there were a number of incidents reported in BWRs in Europe and the USA where power oscillations in the core led to unexpected reactor trips. These oscillations were traced to instabilities caused by coupling of density fluctuations in the coolant with the neutronic response of the fuel. Two types of these coupled neutronic-thermohydraulic instabilities were seen:

- (1) Core-wide reactivity instabilities where the whole core behaved as one and oscillations were in phase across the core; and

- (2) Out-of-phase reactivity instabilities where the power in half the core rises whilst power is reduced in the other half, with average power remaining essentially constant.

ABWRs are designed and operated to avoid regions where these instabilities may occur (for example, the start-up procedure in the UK ABWR where RIPs are started and then control rods are withdrawn is designed precisely to avoid this type of instability – see Chapter 11.5, particularly Figure 11.5-11). However, transients may move the operating envelope into a region where such an instability may occur and, if the reactor fails to scram, power and flow oscillations may occur.

ATWS instability (ATWSI) scenarios (see Section 24.9.1.2) are expected to be bounded by ATWS scenarios with respect to reactor vessel and primary containment integrity. ATWSI analysis is performed to ensure compliance with acceptance criteria for fuel. Therefore, only the PCT results are compared to the acceptance criteria. The bounding event for ATWSI with respect to the acceptance criteria for PCT is Turbine Trip with Bypass [Ref-5].

Table 24.9-1: Provision of HLSFs by Class 2 systems for ATWS events

HLSF	System	PCSR Ref	Notes
1-5 Function of alternative reactivity control	ARI	12.4.3.1	ARI uses the same control rods as normal shutdown but has alternative actuation.
	SLC	12.4.3.2	SLC injects borated water into the primary circuit to shut down the reactor. Power for SLC provided by BBG.
	ATWS-RPT	12.3.5.1	ATWS-RPT reduces core flow to bring negative reactivity into the core.
	FWSTP	12.3.5.2	FWSTP stops feedwater supply in order to lower reactor water level, which reduces circulation of the core flow and then bring negative reactivity into the core.
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	HWBS	14.6.3	HWBS provides the functions to generate actuation signals for the alternative reactivity control systems.
5-3 Function of alternative supporting system	B/B Class 2 EPS	15.4.6	B/B Class 2 EPS supplies power to the second line of safety systems. BBG supports SSCs related to SLC.
	EECW (Class2)	16.3.6	Emergency Equipment Cooling Water System (EECW) supplies recirculation cooling water to BBG.

Table 24.9-1: Provision of HLSFs by Class 2 systems for ATWS events (Continued)

HLSF	System	PCSR Ref	Notes
5-18 Function to maintain internal building environment appropriate for SSCs	Class 2 (A2) HVAC	16.5	Class 2 (A2) HVAC ensures the adequate environmental parameters for SSCs related to SLC are maintained.
	HBCW	16.3.5.3	HBCW provides chilled water for Class 2 (A2) HVAC.

Table 24.9-2: ATWS Mitigation Systems

ATWS Mitigation System	Setpoints
Alternate Rod Insertion (ARI)	<ul style="list-style-type: none"> ATWS High dome pressure Low reactor water level (Level 2)
SLC initiation	<ul style="list-style-type: none"> ATWS High pressure and ATWS permissive for 3 minutes Low reactor water level (Level 2) and ATWS permissive for 3 minutes
ATWS 4 RIPs trip	<ul style="list-style-type: none"> ATWS High dome pressure Low reactor water level (Level 3)
ATWS 6 RIPs trip	<ul style="list-style-type: none"> ATWS High dome pressure (6 RIPs trip automatically 30 seconds after 4 RIPs trip) Low reactor water level (Level 2) (3 RIPs trip at Level 2 immediately and 3 RIPs trip after 6 seconds delay)
Feedwater stop function	<ul style="list-style-type: none"> ATWS High dome pressure and ATWS permissive for 2 minutes for ATWS events.

Limits and Conditions for Operation

The following LCO is identified in addition to those in Section 24.6 and Section 24.7:

The future licensee shall ensure that, during normal power operation, one or more divisions of the following systems are operational even if one division is unavailable due to testing or maintenance and another division is unavailable due to a single failure:

- SLC
- FWSTP
- HWBS

- B/B Class 2 EPS
- BBG
- EECW
- Class 2 (A2) HVAC
- HBCW

The future licensee shall ensure that, during normal power operation, the following SSCs are operational:

- ARI
- ATWS-RPT

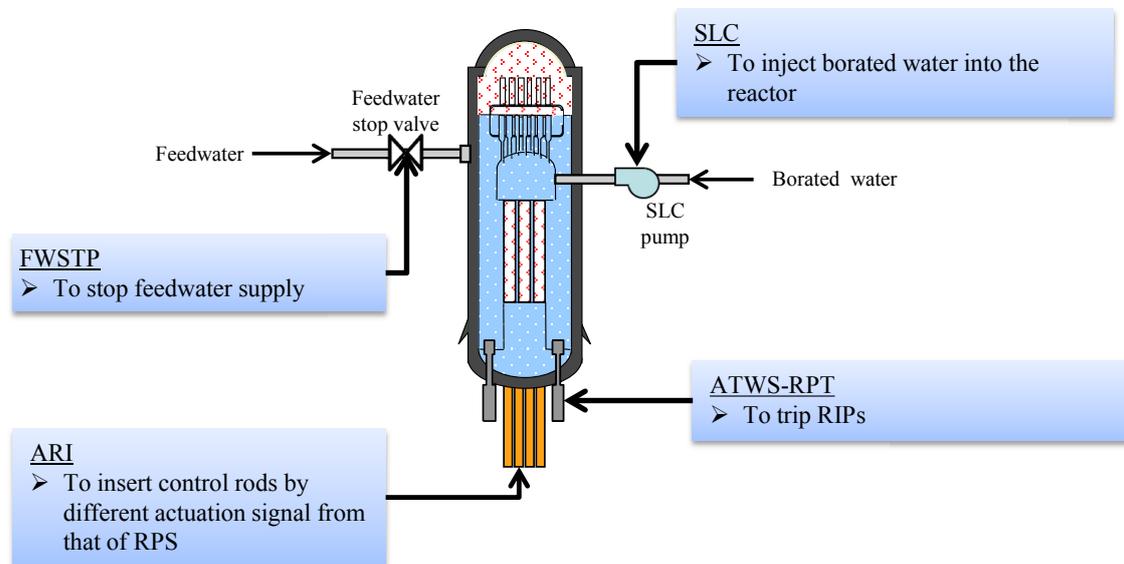


Figure 24.9.1-1: ATWS System Overview

24.9.1.1 ATWS - Main Steam Isolation Valve Closure with Failure to Scram

Fault Schedule Ref: 2.1.1

(1) Description of Fault

During the reactor power operation, the main steam isolation valves are closed by an incorrect signal such as low reactor water level or a misoperation by an operator. The MSIV closure scram signal is correctly generated as designed, but in this ATWS case, for some unspecified reason it is assumed not to deliver its safety function.

(2) Plant Normal Response

A short time after the MSIVs have closed, the ATWS high pressure setpoint is reached, which initiates trip of four of the ten RIPs and runback of the remaining RIPs. After 30 seconds delay from the trip of the four RIPs, the remaining six RIPs also trip. The effect of the trip reduces the core flow and increases core voids, thereby reducing power generation, which limits pressure increase and steam discharge to the suppression pool. The ATWS high pressure signal also causes the actuation of the ARI. The insertion of the control rods is successful in bringing the reactor to hot shutdown.

(3) Analysis of Event

(a) Analysis Assumptions

Analysis conditions are set considering UK practices: for infrequent DB faults such as ATWS events, only equipment providing a Category A Safety Function and claimed in the Fault schedule is credited.

Although no operator actions are credited within 30 minutes from the event initiation for design basis fault analysis in UK, for this event the reactor water level is conservatively assumed to be kept above the top of the active fuel by an operator action within 30 minutes from the event initiation. This is because the assumption of operator action results in a conservative power level during the transient and a conservative suppression pool response. This operator action is not a claim as no Safety Function is associated with it. It therefore does not have a corresponding HBSC.

The initial plant conditions of this analysis are shown in Table 24.9-3 and major plant specifications including setpoints of the safety systems are shown in Table 24.9-4.

Table 24.9-3: Analysis Conditions

Item		Value
Initial Conditions	Thermal power	3926 MW (rated power)
	Core flow	47000 t/h (90 % of rated flow)
	Reactor pressure	7.07 MPa [gauge]
	Steam/Feedwater flow	7640 t/h (rated flow)
	Feedwater temperature	216 °C
	Water level	Normal operating water level
	Initial Suppression Pool Liquid Volume	3580 m ³ (Lower limit of volume)
	Initial Suppression Pool Temperature	35 °C (Upper limit of operating temperature)

Table 24.9-4: Major Plant Specifications Related to Setpoints of the Safety System

Item	Value
ATWS High Pressure Setpoint	7.76 MPa [gauge]
Vessel Level Trips (m above separator skirt bottom)	
Level 3—(L3)	0.57 m
Level 2—(L2)	-0.75 m
Total Number of Safety Valves	15 (One valve with the lowest setpoint is assumed to be unavailable)
Safety Valve Opening Analytic Setpoints (No. of Valves), MPa [gauge]	8.17 (1), 8.24 (4), 8.31 (4), 8.38 (3), 8.45 (3) Analysis values are 3% larger than Nominal setpoint.
Safety Valve Closing Setpoint, % of Opening Setpoints	97 %
Number of SLC Pumps	1 (One division of SLC is assumed to be unavailable due to maintenance)
SLC Injection Rate per Pump	3.15 L/s (189 L/min)
Total SLC Transport Delay Time	270 s
Number of RHR Loops	2 (One division of RHR is assumed to be unavailable due to maintenance)
RHR Service Water Temperature	35 °C (Upper limit of operating temperature)

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent event, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

AC-R2: Pressure on the reactor coolant pressure boundary shall be maintained below 120% of the maximum allowable working pressure.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

The event sequence of this fault is presented in Figure 24.9.1-2 and plant behaviour is presented in Figure 24.9.1-3.

A short time after the MSIVs have closed, the ATWS high pressure setpoint is reached, which initiates trip of four of the ten RIPs. After 30 seconds delay from the trip of the four RIPs, the remaining six RIPs also trip. The effect of the trip reduces the core flow and increases core voids, thereby reducing power generation, which limits pressure increase and steam discharge to the suppression pool. The ATWS high pressure signal also causes the actuation of the ARI. The insertion of the control rods is successful in bringing the reactor to hot shutdown. However, in the case that control rods fail to insert, the reactor is brought to hot shutdown by automatic boron injection by the SLC. Safe shutdown is achieved by the post-accident management described in Section 24.13.5.

(d) Analysis Results

The results of the analysis of ATWS events are shown in Table 24.9-5 and summarised below:

- The maximum fuel cladding temperature is about 794 °C, and so does not exceed the acceptance criterion of 1200 °C. (AC-F5 met with significant margin)
- The calculated total oxidation of the fuel cladding is less than 1%, and so does not exceed the acceptance criterion of 15%. (AC-F4 met with significant margin)
- The peak pressure on the reactor coolant pressure boundary is 8.94 MPa [gauge], and so it does not exceed the acceptance criterion of 10.34 MPa [gauge] (120% of the maximum allowable working pressure). (AC-R2 met with significant margin)
- The peak pressure on the primary containment boundary is 0.134 MPa [gauge], and so it does not exceed the acceptance criterion of 0.310 MPa [gauge] and therefore AC-C1 is met with

significant margin. The peak suppression pool temperature is 100 °C and so it does not exceed the design temperature limit value of 104 °C.

From the above comparisons, all the acceptance criteria regarding the PCT and peak cladding oxidation, peak vessel pressure and containment pressure described above are met for this event.

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the acceptance criteria are met with significant margin.

In the event of a transient with failure of the Class 1 shutdown function, UK ABWR has a number of means of controlling reactivity and of shutting down the reactor:

- Feedwater stop and RIP trip to reduce core activity by increasing voids
- ARI as an alternative means of initiating control rod insertion
- SLC as an alternative means of introducing negative reactivity to the core

In addition, operators can actuate any of these systems in the case of loss of automatic protection.

The normal response to a frequent fault with failure to scram would be that HWBS tries to insert the control rods using ARI and core flow is reduced to reduce the core reactivity by tripping the RIPs (ATWS-RPT) and feedwater (FWSTP). If the control rods still fail to insert, after 3 minutes, HWBS actuates boron injection using SLC. Because SLC takes longer to bring the reactor to hot shutdown than ARI would, it is SLC that is analysed in the design basis analysis, assuming homogeneous mixing of the boron.

However, with less favourable boron solution mixing, the reactor may stay at power longer and could result in increased suppression pool temperature and containment pressure. It is noted that there is significant margin in the containment pressure.

A TRACG model has been generated (Appendix B of Attachment E of [Ref-5]) with sufficient azimuthal nodalisation to investigate the impact of asymmetry on boron injection in the UK ABWR HPCF configuration where the HPCF sparger only covers a 90° portion of the upper plenum. The results calculated by the TRACG 10 theta model, which more realistically captures the impacts of asymmetric injection, show that the reactor power is brought down to hot shutdown values and the suppression pool temperature is bounded by that derived by the ODYN analysis. The TRACG HPCF/SLCS sensitivity study indicates that the suppression pool temperature is not very sensitive to the assumptions of the configuration of HPCF and SLCS and that the UK ABWR is tolerant to asymmetry in boron mixing.

With the significant margins before acceptance criteria are exceeded and the degree of redundancy and diversity, it is determined that the risk from ATWS events is ALARP.

Table 24.9-5: Results Summary of Main Steam Isolation Valve Closure with SLC (Boron Injection)

Figure ID	Max. Neutron Flux (% NBR)	Max. Core Average Surface Heat Flux (% of Initial)	Max. Vessel Bottom Pressure (MPa [gauge])	Max. Bulk Suppression Pool Temperature (°C)	Max. Containment Pressure (MPa [gauge])	PCT (°C)
Figure 24.9.1-3	230	131	8.94	100	0.134	794

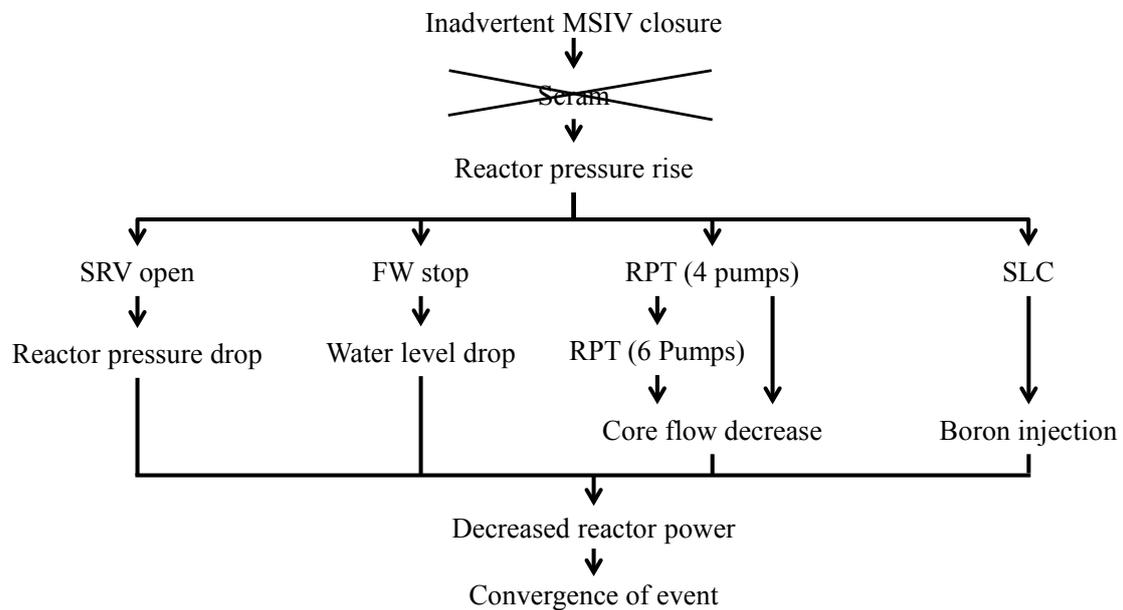


Figure 24.9.1-2: Event Sequence of Main Steam Isolation Valve Closure

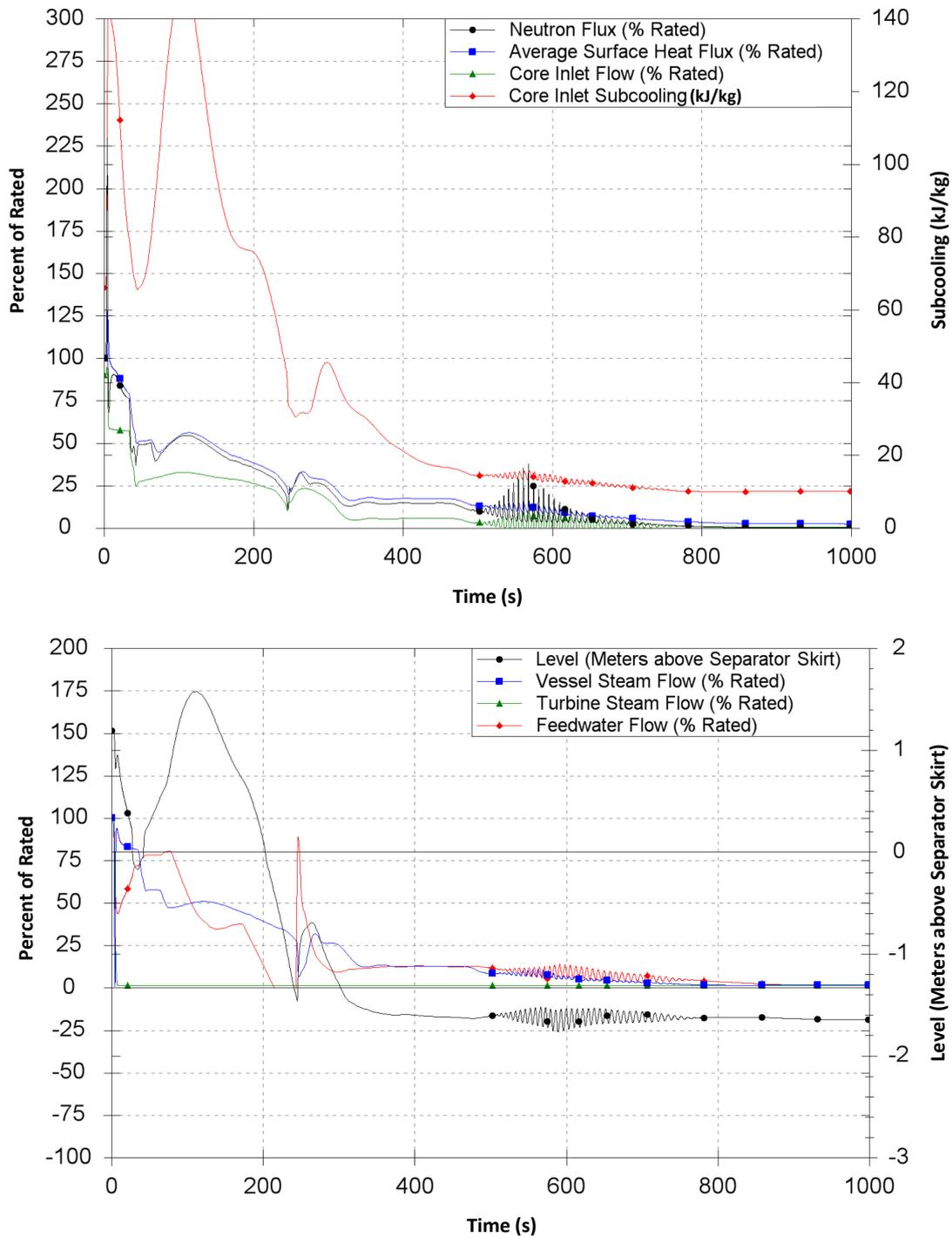


Figure 24.9.1-3: Main Steam Isolation Valve Closure, SLC at EOC

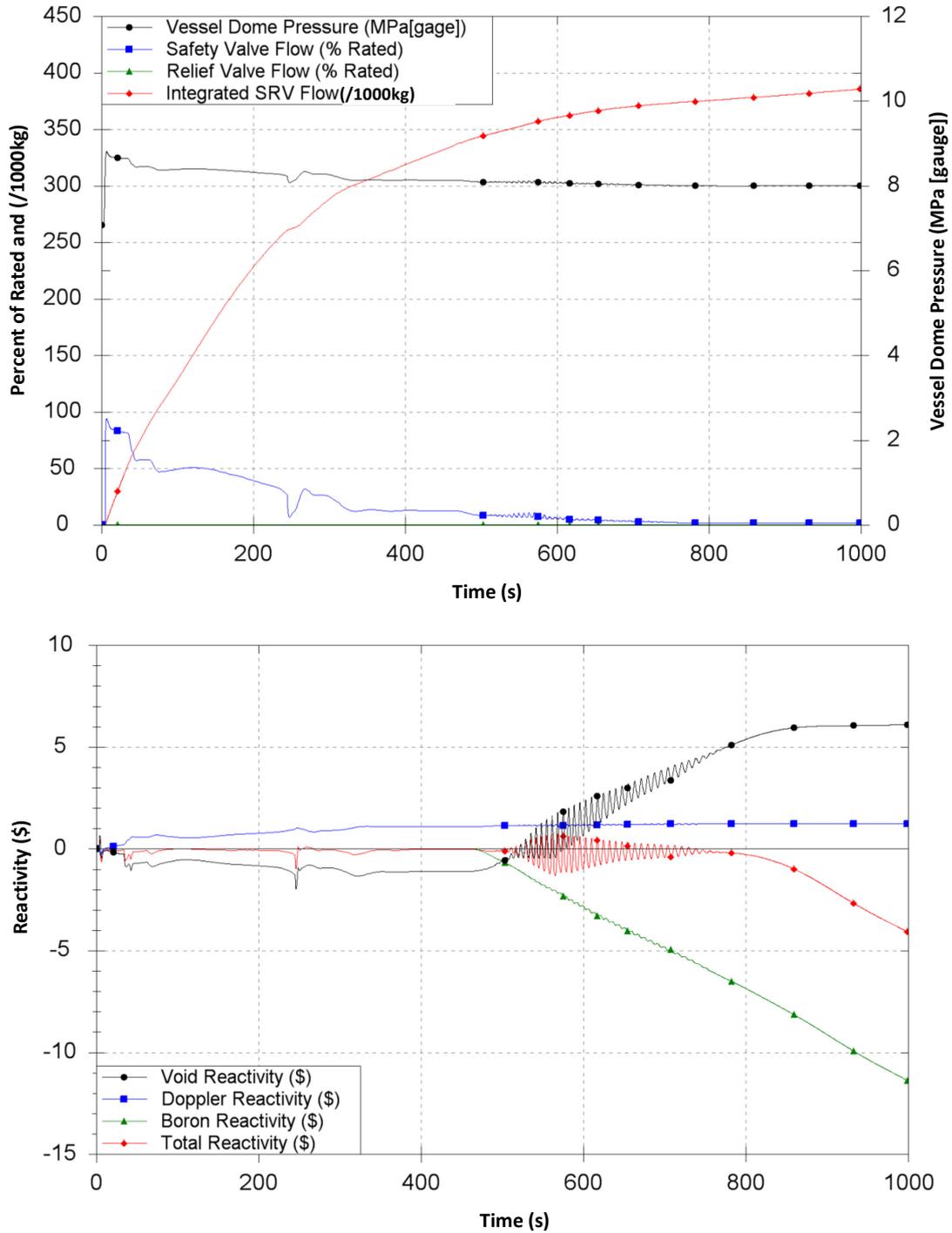


Figure 24.9.1-3: Main Steam Isolation Valve Closure, SLC at EOC(Continued)

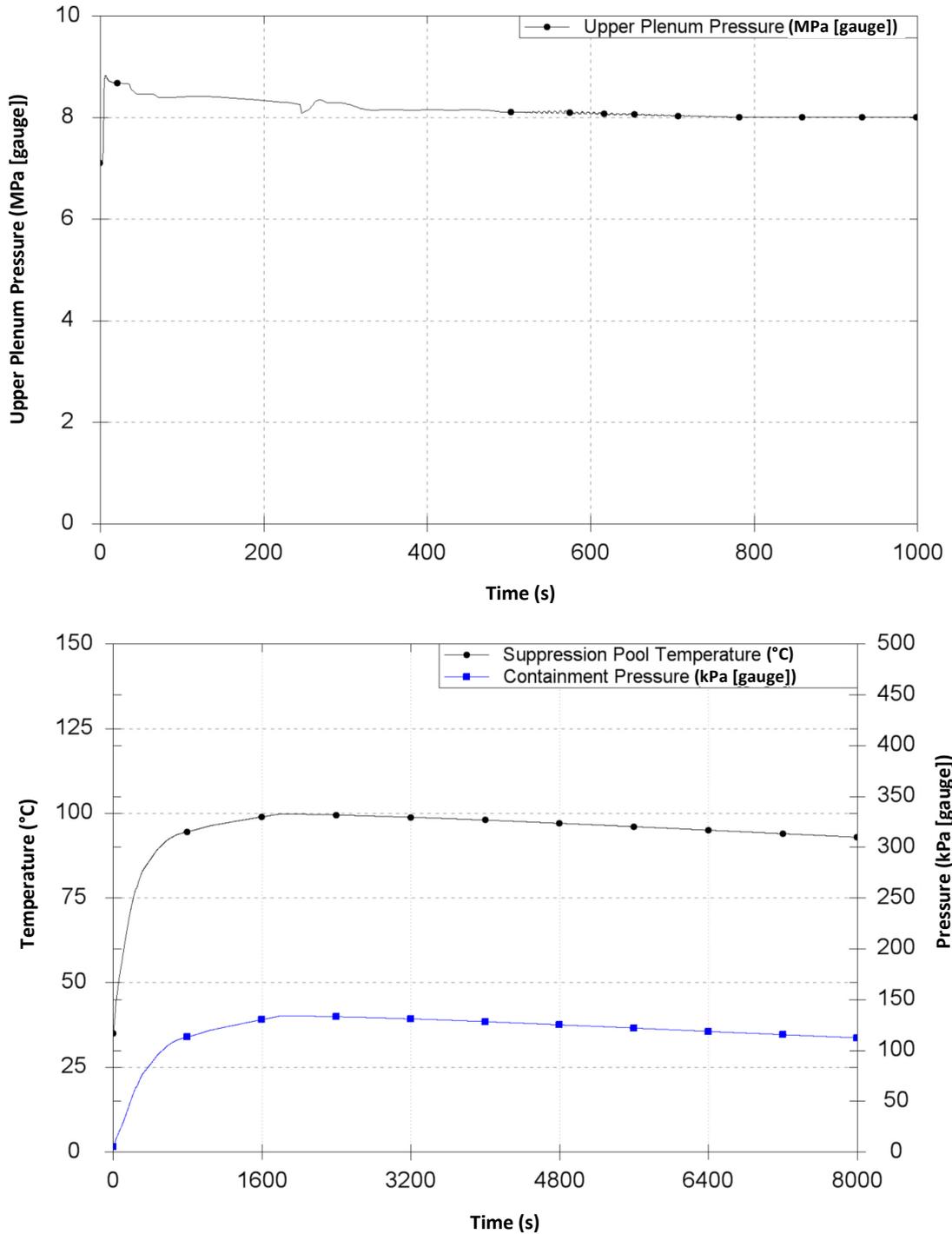


Figure 24.9.1-3: Main Steam Isolation Valve Closure, SLC at EOC (Continued)

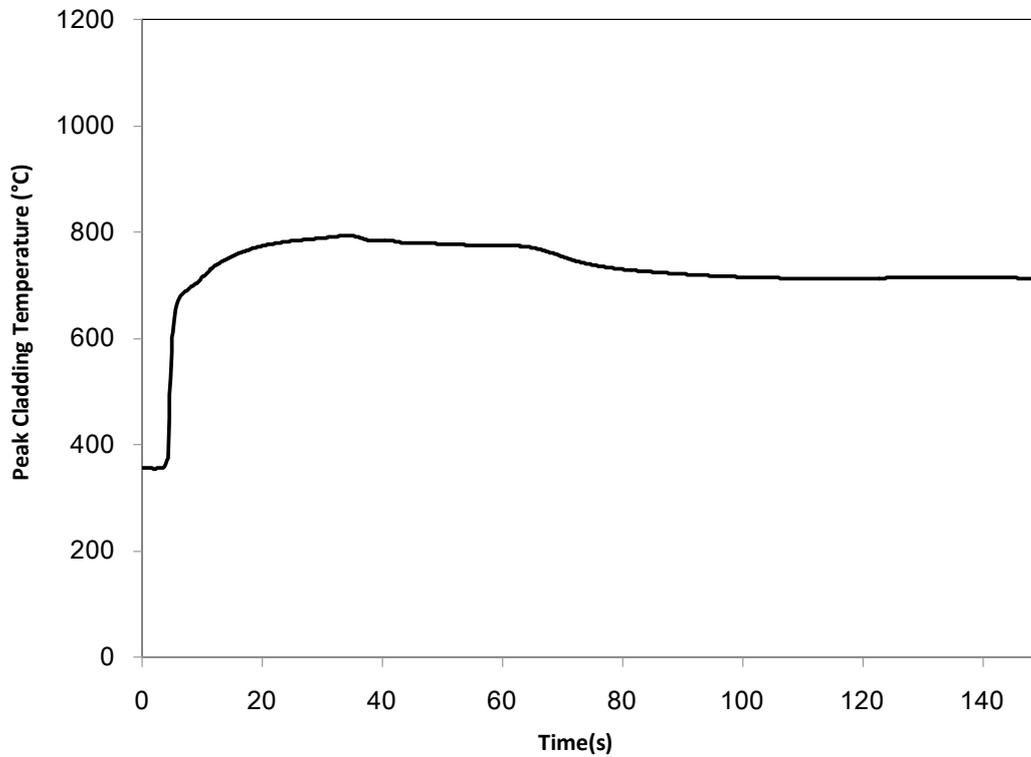


Figure 24.9.1-3: Main Steam Isolation Valve Closure, SLC at EOC (Continued)

24.9.1.2 ATWS Instability

No separate Fault Schedule reference

(1) Description of Fault

Normal UK ABWR operations are design to remain within the stable operating envelope shown in PCSR Chapter 11, Figure 11.5-11. However, as noted earlier, a transient may cause plant operation to enter into the less stable operation region of low core flow and high thermal power and, if the reactor fails to scram, power oscillations due to thermal hydraulic instability may occur.

ATWSI scenarios are expected to be bounded by ATWS scenarios with respect to reactor vessel and primary containment integrity. ATWSI analysis is performed to ensure compliance with acceptance criteria for fuel, in particular, acceptance criteria related to PCT. The most severe event for ATWSI with respect to the acceptance criteria for PCT is Turbine Trip with Bypass.

In this section, the analysis of this bounding ATWSI event is presented. Further detail and some other ATWSI events are described in the Topic Report on DBA [Ref-5].

Protective measures against ATWSI events are the same as the ATWS mitigation systems shown in Table 24.9-1.

(2) Plant Normal Response

Plant normal response is the same as for other ATWS events as described in 24.9.1.1.

(3) Analysis of Event**(a) Analysis Assumptions**

The ATWSI analysis conditions are the same as for ATWS shown in Table 24.9-3 and Table 24.9-4. It is noted that initial core flow is set to 90% rated flow (minimum allowable core flow at rated core power) as a conservative assumption making any power and flow oscillations worse. In addition, in this analysis, the delay time to initiate automatic feedwater stop function is set at 120 seconds.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

(c) Fault Progression

The Turbine Trip with Bypass event occurs at 0 seconds. A short time after the turbine trip, the ATWS high pressure is reached, which initiates trip of four of the ten RIPs and the feedwater stop function. After 30 seconds delay from the trip of the four RIPs, the remaining six RIPs also trip due to the same high pressure setpoint. Because the turbine has tripped, steam is dumped from the turbine bypass to the main condenser, but there is no extraction steam for the feedwater heaters. This results in a long-term supply of cold feedwater, which maximises the core inlet subcooling, and a gradual increase of core power. Power and flow oscillations due to thermal hydraulic instability then occur. At 120 seconds after the ATWS high pressure set point is reached the automatic feedwater stop function reduces the reactor water level. The SLC is needed to bring the core to safe shutdown conditions but is not important to mitigating the oscillations.

(d) Analysis Results

The results of the analysis of ATWSI events are shown in

Table 24.9-6 and Figure 24.9.1-4. The maximum fuel cladding temperature is about 592 °C (AC-F5 met with significant margin) and therefore the increase of the oxide layer thickness on the fuel cladding is very small because the fuel cladding temperature is relatively low (AC-F4 met with significant margin).

(4) Discussion and Conclusions

The ATWSI analysis results demonstrate that the ATWS (ATWS) mitigation systems and operator action for the UK ABWR are successful in mitigating the consequences of ATWS instability events. Therefore, the acceptance criteria regarding fuel described above are met for this event.

The discussion on ALARP for ATWSI events is the same as for ATWS events above.

Table 24.9-6: Results Summary for Turbine Trip with Bypass without Scram

Item	Value
Peak Cladding Temperature (°C)	592

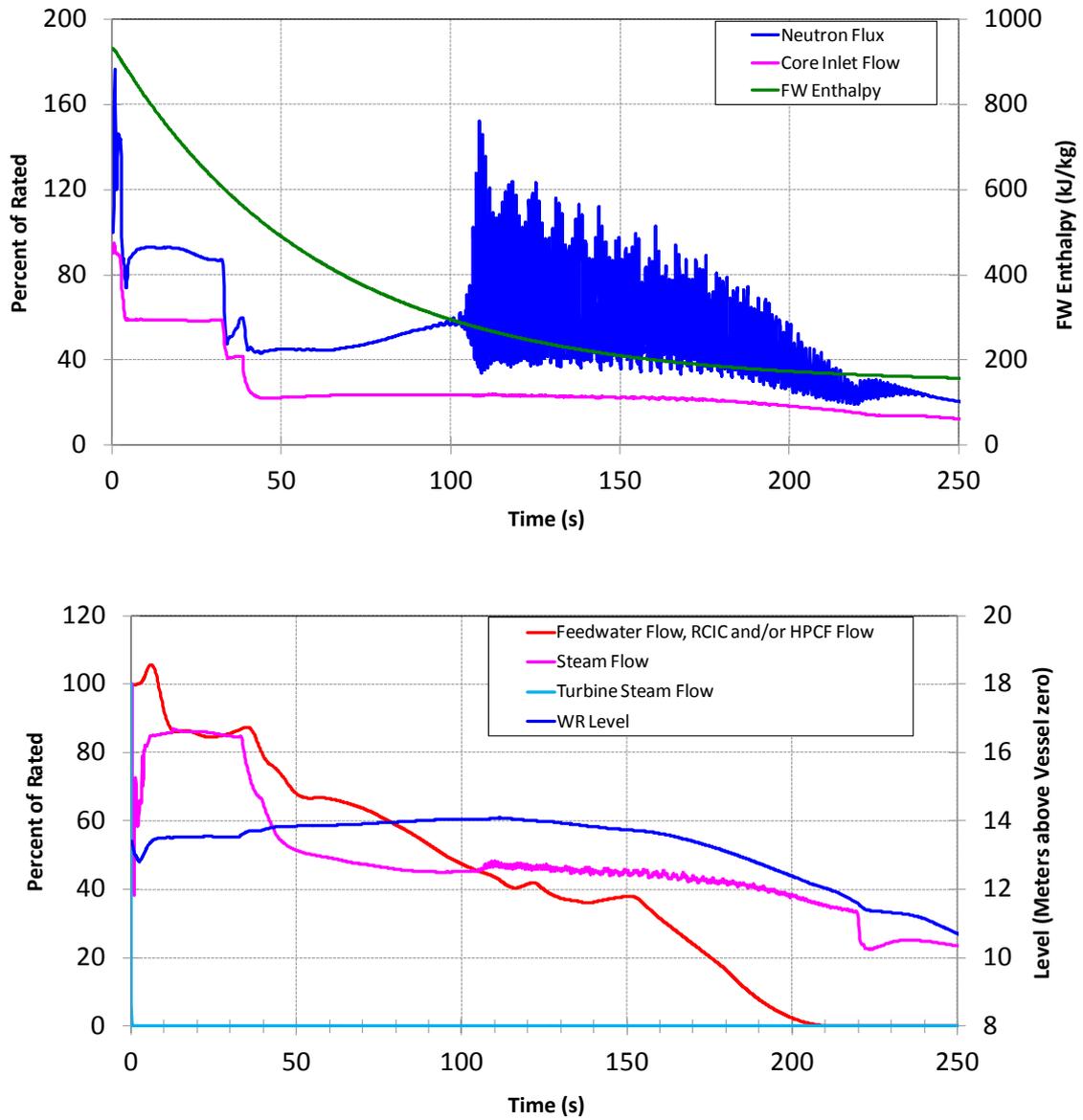


Figure 24.9.1-4: Turbine Trip with Bypass without Scram

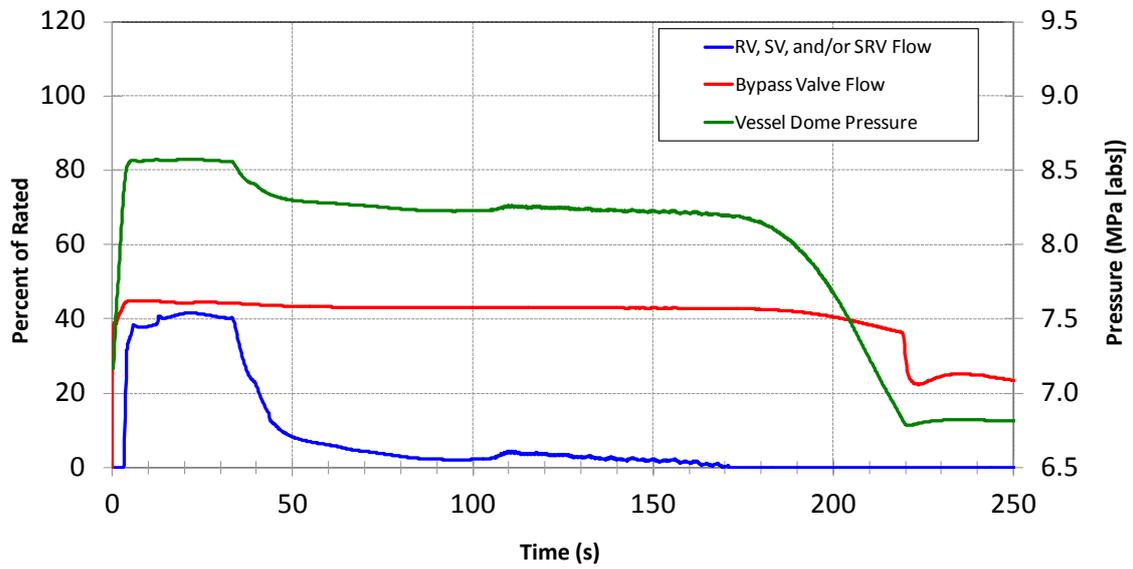


Figure 24.9.1-4: Turbine Trip with Bypass without Scram (Continued)

24.9.2 Station Blackout (SBO)

Supply of off-site electrical power is an important element for safe operation and accident recovery of the UK ABWR. Therefore, loss of off-site power (LOOP) is an initiating event to be considered in the design basis analysis. In addition to the consideration of LOOP as the initiating event (see Section 24.7.3), LOOP with a common cause failure (CCF) of the emergency diesel generators (EDGs) is considered as a DB fault to demonstrate the fault tolerance of the design and the robustness of safety measures against the LOOP events.

The following assumed LOOP frequency figures are used for the UK ABWR generic site in this GDA assessment:

- Short term LOOP of 2 hours duration $5 \times 10^{-2} /y$
- Medium term LOOP of 24 hours duration $5 \times 10^{-3} /y$
- Long term LOOP of 168 hours duration $5 \times 10^{-5} /y$

Based on these assumed frequencies, short and medium term LOOP initiating events are treated as frequent faults and long term LOOP initiating events as infrequent faults.

In the light of their frequencies, the following events consisting of LOOP plus CCF of EDGs are analysed as follows:

- (i) Short term LOOP with CCF of EDGs is considered as an infrequent DB fault (Short term SBO) (Fault Schedule Ref: 5.1.1)
- (ii) Medium term LOOP with CCF of EDGs is considered as an infrequent DB fault (Medium term SBO) (Fault Schedule Ref: 5.2.1)
- (iii) Long term LOOP with CCF of EDGs is considered as a BDB fault (Long term SBO - see Chapter 26) (Fault Schedule Ref: 5.3.1)

In addition,

- (iv) Long term LOOP with CCF of EDGs and loss of Back-up Building Generators (BBGs) is also considered as a BDB fault (Fault Schedule Ref: 5.3.4)

In addition, the short term SBO is the same as the first 2 hours of the medium term SBO. Therefore, the short term SBO is represented by the medium term SBO. Consequently, this section only describes analysis of the medium term SBO event.

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

With the loss of both off-site power and EGDs, the plant relies on the Class 1 RCIC and Class 2 systems powered by the BBGs to supply the HLSFs relating to heat removal in the short term and medium term.

Table 24.9-7 shows the provision of HLSFs in response to a SBO event.

Table 24.9-7: SSCs providing HLSFs for SBO events

HLSF	SSC	PCSR ref	Notes
1-3 Emergency shutdown of the reactor	CRD (Class 1)	11.5.2, 12.4.3.1	
2-1 Functions to cool reactor core	RCIC SRV (Class 1)	13.4 12.3.5.2	RCIC is powered by a steam turbine and only requires DC power to operate. Batteries have 24 hour life. RCIC stops if reactor is depressurised.
2-2 Function of alternative fuel cooling	RDCF FLSS (Class 2)	16.7.3.3 16.7.3.1	RDCF depressurises reactor so that FLSS can function. Power for RDCF is provided by B/B Class2 DC power supply system. Power for FLSS is provided by BBG.
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to RDCF and FLSS.
3-1 Functions to remove residual heat after shutdown	RHR (Class 1)	12.3.5.4	RHR is used after restore of off-site power for safe shutdown.
	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to control SSCs related to RHR.
3-2 Functions of alternative containment cooling and decay heat removal	AC FCVS (Class 2)	13.3.3.4	Heat rejected by feed and bleed with containment venting via AC or FCVS.
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to AC and FCVS.
4-2 Functions to prevent overpressure within the reactor coolant pressure boundary	SRV (Class 1)	12.3.5.2	Safety valve function of SRVs
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to generate actuation signals for the engineered safety features (RCIC) and reactor shutdown system (CRD scram).

Table 24.9-7: SSCs providing HLSFs for SBO events (Continued)

HLSF	SSC	PCSR ref	Notes
5-2 Supporting functions especially important to safety	Class 1 EPS (Class 1)	15.3	Class 1 DC batteries supply power to RCIC.
5-3 Function of alternative supporting system	B/B Class 2 EPS (Class 2)	15.4.6, 15.4.8.4	B/B Class 2 EPS including B/B Class2 DC power supply system supplies power to the second line of safety systems. BBG supports SSCs related to alternative fuel cooling and alternative long term heat removal.
	EECW (Class 2)	16.3.6	EECW supplies recirculation cooling water to BBG auxiliaries.
	DAG (Class 3)	15.5.5	DAG supplies power to any one division of Class 1 EPS during SBO event as a defence in depth measures to support RHR and its associated systems. Note that DAG is not credited in DBA.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 2 (A2) HVAC	16.5	Class 2 (A2) HVAC ensures the adequate environmental parameters for SSCs related to SLC are maintained.
	HBCW	16.3.5.3	HBCW provides chilled water for Class 2 (A2) HVAC.

Limits and Conditions for Operation

The following LCO is identified in addition to those in Section 24.6 and Section 24.7:

The future licensee shall ensure that, during normal power operation, no more than one division of the following systems and their support systems in the same division shall be subject to testing or maintenance:

- FLSS
- AC and FCVS treated as one system
- HWBS
- B/B Class 2 EPS
- BBG
- EECW
- Class 2 (A2) HVAC

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

- HBCW

The future licensee shall ensure that, during normal power operation, the following SSCs are operational:

- RDCF

NOT PROTECTIVELY MARKED

24.9.2.1 Medium term SBO

Fault Schedule Ref: 5.2.1

(1) Description of Fault

The fault is initiated by loss of off-site power as in Section 24.7.3. However, apart from RCIC, Class 1 SSCs are unavailable because of CCF of the EDGs. For all possible LOOP events, the UK ABWR has three divisional EDGs whose on-site fuel tank capacity lasts more than 7 days (168 hours) to reduce the probability of station blackout (SBO). In addition, even for the SBO events, the UK ABWR has core cooling that is independent of AC electrical power, alternate water injection supported by alternate AC power, and alternate long-term heat removal. AC-independent core cooling is achieved by the RCIC (with 8 hours capability). The alternate water injection is achieved by the FLSS from the backup building powered by the BBGs which can supply more than 7 days power. In addition, the alternate water injection is achieved by the FLSR. Also, alternate long-term heat removal is achieved by the RHR system recovered by a Diverse Additional Generator (DAG) or containment venting powered by the BBGs.

This fault bounds:

- Short term SBO (Fault Schedule Ref: 5.1.1)

(2) Plant normal response

The plant normal response to this event is to automatically scram the reactor and automatically initiate the RCIC as in the fault analysis.

(3) Analysis of Event

The analysis of this fault is presented in two parts:

- Thermal-hydraulic analysis
- Dose evaluation

(I) Thermal-hydraulic analysis

After the station blackout occurs, the AC-dependent safety systems and components are all assumed to fail. The DC batteries supply power to the facilities required for accident management for up to 24 hours and AC power is not available for 24 hours. In a typical emergency operating procedure, in the case of SBO with failure of the Diverse Additional Generator, the operators depressurise the RPV within 8 hours and cooling water is injected into the RPV using the low pressure injection system (e.g. FLSS) after depressurisation. In addition, heat removal is implemented by containment venting when the PCV pressure reaches 310 kPa [gauge]. The suppression pool is cooled by the RHR system

in pool cooling mode when electric power is recovered after 24 hours. When the suppression pool temperature is sufficiently low, heat removal from the reactor core is implemented by the RHR system in shutdown cooling mode.

(a) Analysis Assumptions

The analysis conditions are listed below. Further details of the analysis conditions are described in section 6.2.2 of the Topic Report on SBO Analysis [Ref-16]

- (i) All AC-dependent Class 1 safety systems and components are assumed to fail.
- (ii) The DC batteries supply power to the facilities required for operation for up to 24 hours
- (iii) AC power from off-site and EDGs is not available for the first 24 hours.
- (iv) SRVs automatically open or close to maintain the RPV pressure.
- (v) The reactor water level is maintained at the proper level by water injection using the RCIC or FLSS.
- (vi) The reactor is depressurised by operator action.
- (vii) Heat removal is achieved by containment venting when the pressure in the containment reaches the maximum allowable working pressure.
- (viii) Heat removal from the core is achieved by the RHR system (shutdown cooling mode), when electric power is recovered after 24 hours.
- (ix) RCIC is assumed to be available for up to 8 hours. One division of each Class 2 system in Table 24.9-7 is assumed to be available.

The successful termination of the event relies on a number of operator actions summarised as follows:

- (i) The reactor is depressurised by manually opening 2 SRVs at 8 hours after LOOP.
- (ii) The FLSS begins injecting to the RPV to maintain reactor water level after the RPV is depressurised. (Items (i) and (ii) together are covered by HBSC HF FLSS 2-2.1 – see Chapter 27, Appendix A)
- (iii) Containment wetwell venting is initiated when the PCV pressure reaches 310 kPa [gauge].
- (iv) Containment venting is terminated after 24 hours and remains closed afterwards. (Items (iii) and (iv) together are covered by HBSC HF AC 3-2.1 - see Chapter 27, Appendix A)
- (v) The RHR pool cooling mode is initiated after 24 hours.
- (vi) The RHR is switched to shutdown cooling mode when the suppression pool temperature decreases below 100 °C. (Items (v) and (vi) together are covered by HBSC HF RHR 3-1.4 – see Chapter 27, Appendix A)

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is an infrequent fault, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

AC-R2: Pressure on the reactor coolant pressure boundary shall be maintained below 120% of the maximum allowable working pressure.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

AC-D5: Dose to workers should be less than 500 mSv.

AC-D6: Dose to members of the public should be less than 100 mSv.

(c) Fault Progression

The event sequence during Medium term LOOP with CCF of EDGs is shown in Figure 24.9.2-1.

The high drywell temperature is caused by maintaining high RPV pressure. With this elevated RPV pressure, the sustained heat load from the RPV wall to the drywell atmosphere drives up the drywell temperature. After the reactor is depressurised at 8 hours, the temperature increase in the drywell stops and the temperature is kept below the drywell design temperature (171 °C). The temperature in the wetwell and suppression pool is also increased by the release of RPV coolant through the SRVs and RCIC turbine. Due to actuation of PCV venting, the pressure in the drywell and wetwell is maintained below the maximum allowable working pressure (310 kPa [gauge]) and the temperature in the wetwell and the suppression pool are kept below saturation temperature. The suppression pool is cooled by the RHR system in pool cooling mode when electric power is recovered after 24 hours. Subsequently, when the S/P temperature decreases below 100 °C, reactor core heat removal is achieved by reactor depressurisation and the RHR system in shutdown cooling mode. Thus the reactor core is cooled.

(d) Analysis Results

The key results for this SBO event are provided in Table 24.9-8 and Figure 24.9.2-2 to Figure 24.9.2-5.

The reactor core is maintained fully covered due to water injection by the RCIC and FLSS. The peak cladding temperature and cladding oxidation rate do not increase from their initial values. (AC-F5 and AC-F4 met with significant margin)

The reactor pressure is controlled by the SRVs and is maintained below 120% of the maximum allowable working pressure (10.34 MPa [gauge]). (AC-R2 met with some margin)

Due to the containment venting, the drywell and wetwell pressures are maintained below the containment maximum allowable working pressure. The vent flow is sufficient to control the containment pressures below the maximum allowable working pressure (310 kPa [gauge]). (AC-C1 met)

The peak drywell temperature (168 °C) is also kept below the design limit value of 171°C.

Both peak pool temperature (143 °C) and peak wetwell temperature (144 °C) exceed the pool and wetwell design limit value of 104 °C. However, the ultimate capacity of the UK ABWR Reinforced Concrete Containment Vessel (RCCV) is :

- Temperature : 200°C [Ref-28],
- Pressure : 2Pd (Pd : 310kPa) [Ref-28].

Therefore, the integrity of the PCV boundary is maintained.

Table 24.9-8: Results Summary for SBO Analysis

Parameters	Values
Peak Cladding Temperature	No increase from initial value
Cladding Oxidation Rate	No increase from initial value
Peak Reactor Pressure	8.26 MPa [abs]
Peak Drywell Pressure	307 kPa [gauge]
Peak Drywell Temperature	168 °C
Peak Wetwell Pressure	310 kPa [gauge]
Peak Wetwell Airspace Temperature	144 °C
Peak Suppression Pool Temperature	143 °C

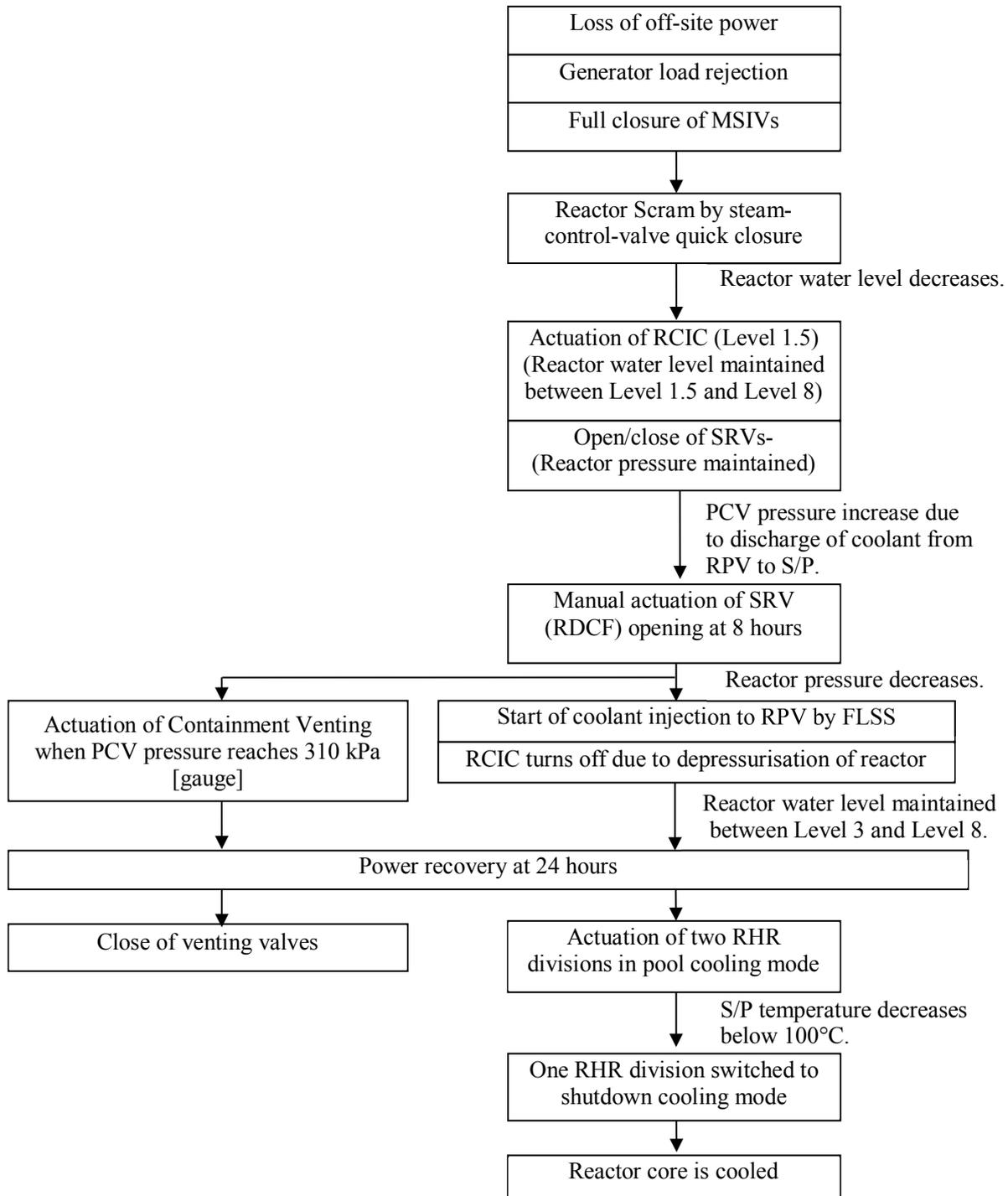
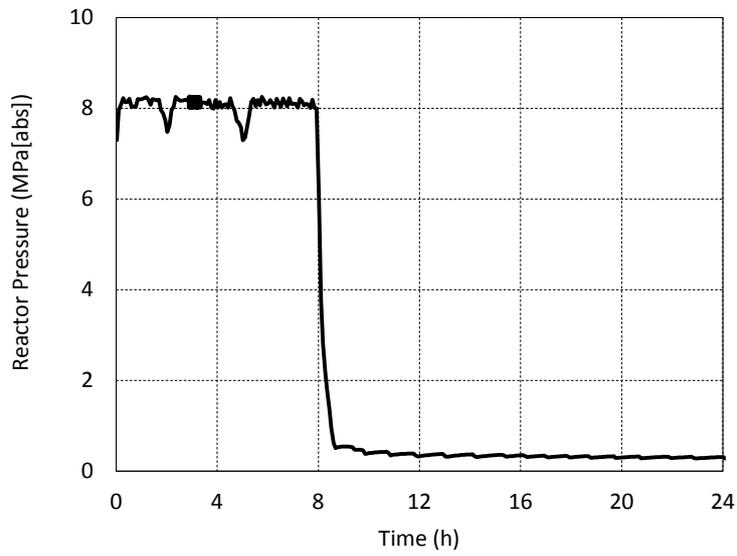


Figure 24.9.2-1: Event Sequence for Medium Term LOOP with CCF of EDGs



(a) Reactor Pressure

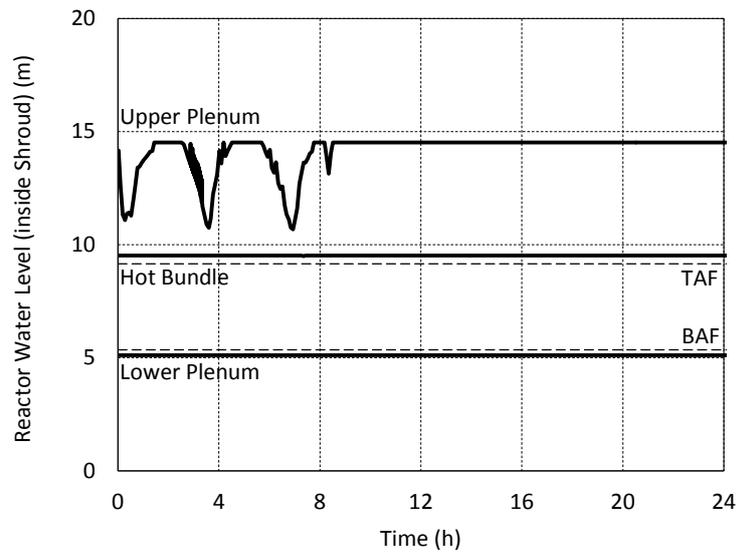
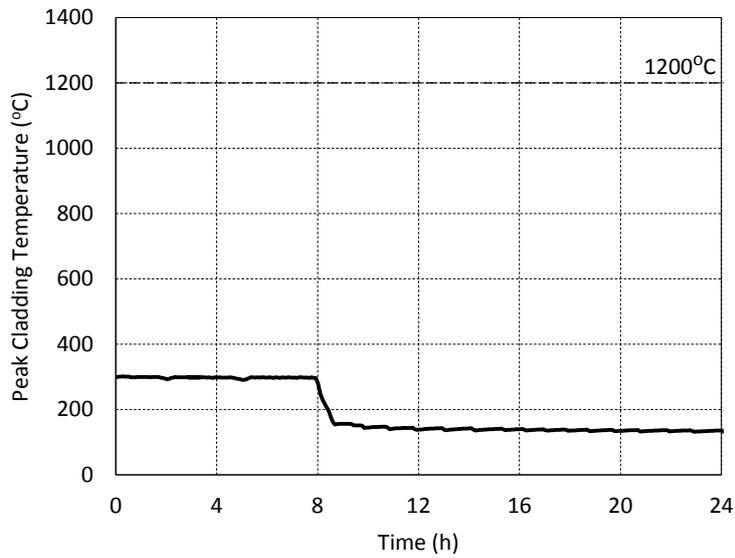


Figure 24.9.2-2: Reactor Pressure and Water Level Transients during Medium Term LOOP with CCF of EDGs



(e) Peak Cladding Temperature

Figure 24.9.2-3: Peak Cladding temperature Transient during Medium Term LOOP with CCF of EDGs

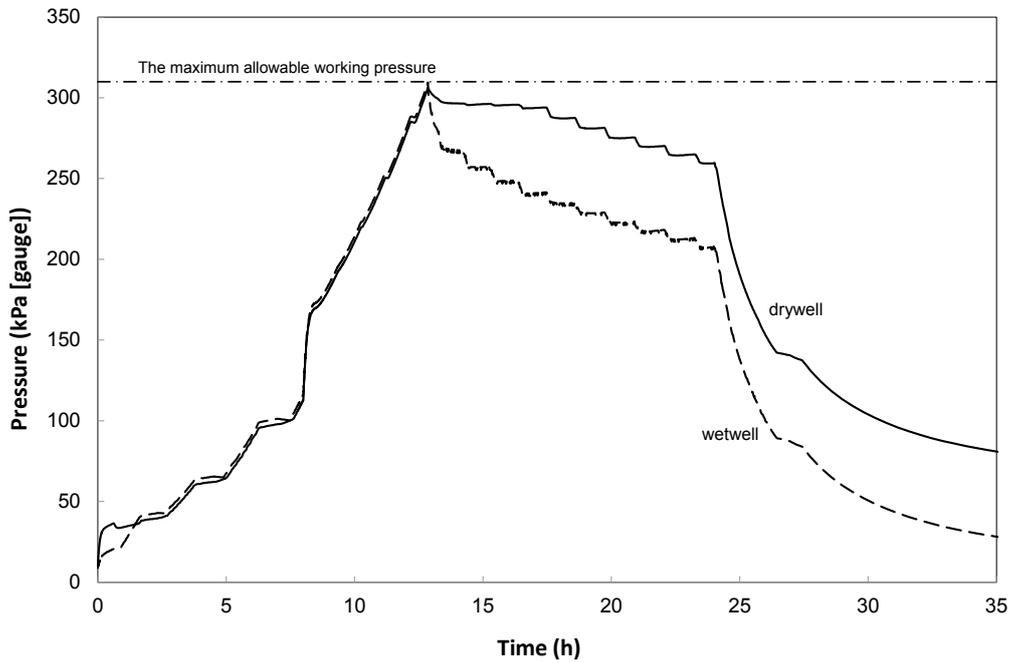


Figure 24.9.2-4: Pressures Transient in the Drywell and Wetwell during Medium Term LOOP with CCF of EDGs

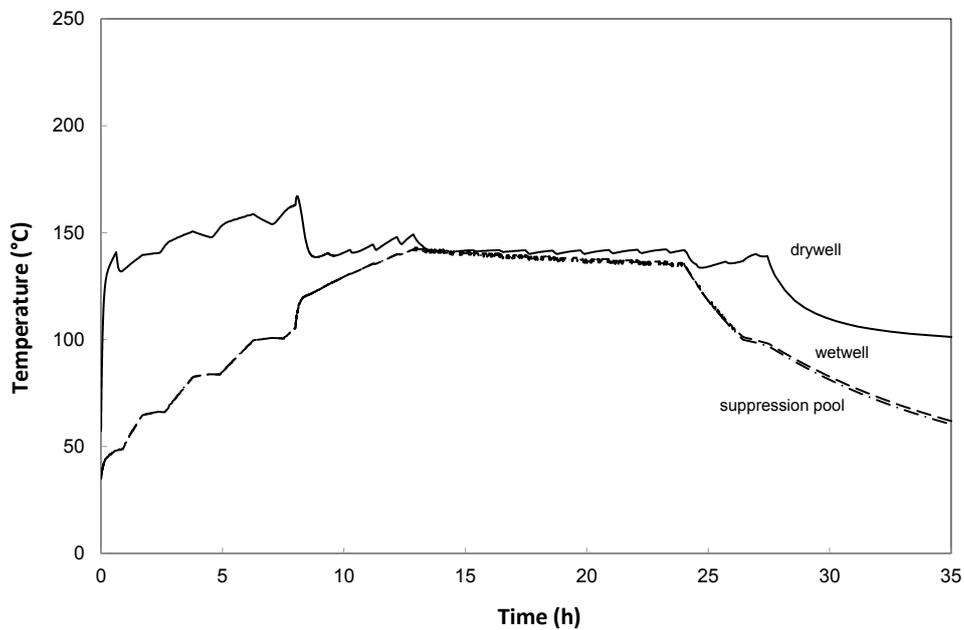


Figure 24.9.2-5: Temperature Transients in the Drywell, Wetwell and Suppression Pool during Medium Term LOOP with CCF of EDGs

(II) Dose Evaluation

(a) Analysis Assumptions

The release and transport pathway for radionuclides assumed for the dose analysis for this event is shown in Figure 24.9.2-6. The SRVs automatically open to release the RPV steam into the suppression pool. The radionuclides are released to the environment via the suppression pool and through the Vent line to the stack. The following assumptions and conditions form the basis for the analysis.

- During an SBO, there is no fuel damage due to operation of Class 2 SSCs.
- An iodine spike is considered during the event, with a severity that depends on the differential depressurisation ratio. The differential depressurisation ratio is based on the calculated reactor pressure shown in Figure 24.9.2-2 (a).
- The containment venting and radionuclides release are assumed to take place 12.8 hours after the initiating event.

(b) Release Mass and Source Term

The release duration for this SBO sequence is the duration of the venting operation. The mass of steam released from the Vent line is about 5.12×10^5 kg over a period of 24 hours.

The concentration of nuclides in steam for this SBO sequence is based on the source terms listed in [Ref-29]. The amount of iodine that is released from the fuel in the spike is determined based on the depressurisation of core. The core pressure reduces to approximately atmospheric pressure based on the thermal hydraulic analysis. In practice, it is conservatively assumed that 100% of the iodine is released [Ref-18].

The total activity release from the vent line to the environment was calculated using the following equation:

$$\text{Total released activity} = (\text{steam mass}) \times (\text{steam concentration}) + (\text{iodine spike}) \times (\text{carryover})$$

The extent of carryover of the iodine from the coolant was assumed based on the Operational Experience (OPEX) data. The carryover of noble gas was assumed to be negligible.

In this event, the reactor steam is released to the suppression pool through the instantaneous opening of the SRVs, and all the radionuclides in the iodine spike were assumed to be instantaneously and homogeneously mixed with the containment atmosphere. As steam released from the SRVs to the suppression pool was fully quenched in the cool pool water, almost all of the radioactive nuclides released with steam were deposited in the suppression pool water. This analysis assumed a

decontamination factor for elemental iodine and other types of nuclides based on the suppression pool scrubbing behaviour. The retention of noble gases was assumed to be negligible.

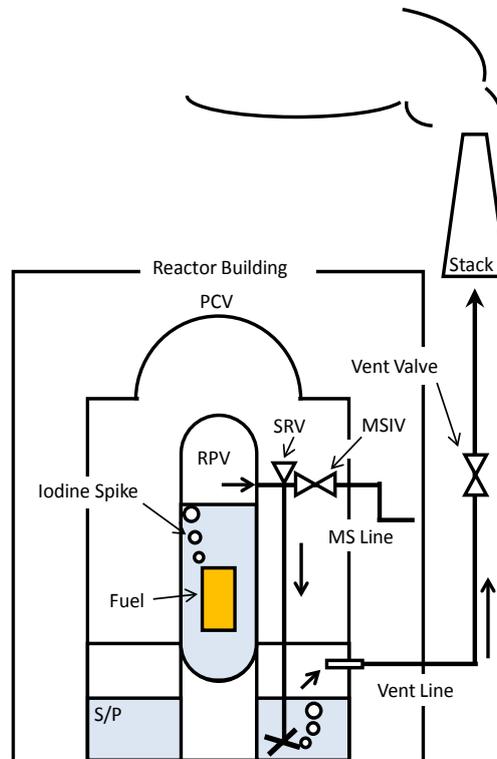


Figure 24.9.2-6: Release Pathway for Radionuclides

(c) Analysis Results

The radioactivity from radionuclides released to the environment due to this fault sequence is shown in Table 24.9-9. Public and worker doses are evaluated to be lower than the AC-D6 and AC-D5 acceptance criteria values respectively, and are below the BSO values. In addition, if containment venting is actuated at the later time when PCV pressure reaches 2Pd (620 kPa [gauge]), the calculated dose is essentially the same as for 1Pd. Since for both cases (containment venting actuation at either 1Pd or 2Pd) the evaluated doses are below the BSO, it is concluded that containment venting can be actuated when the containment pressure is between 1 Pd and 2 Pd. For both cases, there is plenty of time before actuation of containment venting is required to allow the operators to take the necessary actions.

Table 24.9-9: Doses to Exposed Persons from SBO event (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	2.9E-03	1.3E-03	9.0E-04	AC-D6 (BSL): 1.0E+02 BSO: 1.0E-02
On-site (Control Room)	-	-	7.6E-04	AC-D5 (BSL): BSL: 5.0E+02 BSO: 1.0E-01

(4) Discussion and Conclusions

The results of the analysis demonstrate that the acceptance criteria relating to fuel, the reactor pressure boundary, containment and radiation exposure described above are satisfied for the design basis SBO event. Therefore, the fault tolerance of the design and the robustness of safety measures are confirmed against SBO events.

Although the Medium term SBO event is treated as an infrequent DB event, the acceptance criteria are shown to be met using Class 2 SSCs to provide the relevant HLSFs. Normally, the NSEDPs require that the principal protection against DB faults should be Class 1. However, [Ref-34] provides evidence that, in the particular case that the initiating event for an infrequent DB fault involves the CCF of Class 1 SSCs (as in the case of SBO), it is ALARP to rely on the Class 2 diverse provision of the corresponding HLSFs.

24.9.3 Common Cause Failures of C&I systems, Electrical Distribution Systems and Essential Services and Support Systems

The following additional events have been identified by the study of CCF of C&I systems, electrical distribution systems and essential services and support systems in Section 24.4.4.2. The safety case for CCFs which demonstrates the robustness of the design against CCFs of support systems is given in [Ref-34]. The event (ii) to (x) listed below are caused by failure of Class 1 function and they are designated as infrequent events. The event (i) is caused by failure of a Class 3 function and it is designated as a frequent event.

CCF of C&I systems

- (i) All Control Rod insertion (Fault Schedule Ref: 11.1)
- (ii) Inadvertent opening of all ADS (Fault Schedule Ref: 11.2)
- (iii) Inadvertent start-up of all injection systems (Fault Schedule Ref: 11.3)
- (iv) Inadvertent opening of all ADS due to spurious failure of Class 1 SSLC (Fault Schedule Ref: 11.4)
- (v) Inadvertent MSIV closure due to spurious failure of Class 1 SSLC (Fault Schedule Ref: 11.5)

CCF of Electrical Power Supply systems

- (vi) M/C power supply failure on electrical CCF (Fault Schedule Ref: 11.8.1)
- (vii) D/C power supply failure on electrical CCF (Fault Schedule Ref: 11.9.1)

CCF of Essential Services and Support systems

- (viii) Loss of all RCW (Fault Schedule Ref: 11.10.1)
- (ix) Loss of all RSW (Fault Schedule Ref: 11.11.1)
- (x) Loss of all Class 1 HVAC (Fault Schedule Ref: 11.12.1)

In this section, analysis results for the “Inadvertent opening of all ADS” event and “All rods insertion” event are presented as a representative case to demonstrate robustness of the safety design for CCF events. The detailed evaluations are reported in attachment K of the Topic Report on DBA [Ref-5].

No HLSFs for events caused by CCF of essential support systems are identified in addition to those in Section 24.7, Section 24.8, Section 24.9.1, Section 24.9.2 and Section 24.12. Therefore, no LCOs are identified in addition to those in Section 24.6, Section 24.7, Section 24.8, Section 24.9.1 and Section 24.9.2.

Analysis conditions are the same as in Table 24.6-2. Details of trip parameters and other conditions are shown in Table 24.9-10 and Table 24.9-11.

Table 24.9-10: Analysis Setpoints of Safety System

Item	Analysis Conditions	Note
High reactor pressure scram	7.62 MPa [gauge]	–
High neutron flux scram in terms of neutron flux	125%	–
Large axial peaking power difference scram	140%	–
Turbine main steam stop valve closure scram	85% stroke position	100% as full open
High D/W pressure scram	13.8 kPa [gauge]	–

*The 2 out of 4 logic is applied for Class 1 safety systems, as described in PCSR Chapter 14. Therefore the system maintains the safety functions even when considering single failure and maintenance.

Table 24.9-11: Major Plant Specifications Related to Other Systems

Item	Analysis Condition	Note
Scram insertion time	1.71 s at 60% of full stroke 3.70 s at 100% of full stroke	The setpoints of the scram insertion time at the rated pressure are 1.44 seconds or less at 60% insertion of full stroke and 2.80 seconds or less at 100% insertion of full stroke. However, in analysing abnormal operational transients, 1.71 seconds at 60% insertion and 3.70 seconds at 100% insertion are used. The dependence of the control rod drive system on the reactor pressure was taken into consideration to determine these values.
High reactor water level (turbine trip)(Level 8)	+1.73 m from the bottom of separator skirt	This function is used if it is relevant to the fault.
Safety Relief Valve setpoints (Safety function)	1st stage : 8.17 MPa [gauge] 2 valves 2nd stage : 8.24 MPa [gauge] 4 valves 3rd stage : 8.31 MPa [gauge] 4 valves 4th stage : 8.38 MPa [gauge] 3 valves 5th stage : 8.45 MPa [gauge] 3 valves	Analysis conditions are 3% larger than nominal setpoints.
ADS function SRV	7 valves	Function initiated by high D/W pressure or low reactor water level (Level 1).
Motor Driven Reactor Feed Pump (MD-RFP) flow rate per pump	27.5% of the rated feedwater flow	The number of MD-RFPs is two.
HPCF flow rate per pump	182 m ³ /h at 8.12MPa[dif] 727 m ³ /h at 0.69 MPa[dif]	<ul style="list-style-type: none"> • MPa[dif] is a unit of differential pressure between the reactor pressure and the HPCF water source pressure • The number of HPCFs is two.
RHR heat exchanger K-Factor per loop in containment cooling mode	5.88×10^5 W/°C	The number of RHRs is three.

24.9.3.1 Inadvertent Opening of All ADS

Fault Schedule Ref: 11.2

(1) Description of Fault

Inadvertent opening of the ADS SRVs is initiated by CCF of the protection system and all of the ADS SRVs open. Though the behaviour of this event is similar to “Inadvertent opening of an SRV”, the numbers of opening SRVs are greater in this case. The opening of all ADS SRVs allows steam to be discharged into the suppression pool and the suppression pool temperature is increased. The sudden increase in the rate of steam flow leaving the reactor vessel causes a reactor depressurisation transient.

(2) Plant Normal Response

The main protection against the fault is described below:

- (i) Scram is initiated on high S/P temperature or high D/W pressure (Class 1).
- (ii) The RHR is initiated automatically on high S/P temperature and starts S/P cooling (Class 1).

(3) Analysis of Event**(a) Analysis Assumptions**

The analysis conditions are listed in (i) to (viii) below. Further details of the analysis conditions are described in Attachment K, Section K.4.1 of the Topic Report on DBA [Ref-5].

- (i) The initial conditions of the analysis are shown in Table 24.6-2.
- (ii) 7 SRVs are opened at 0.0 second by inadvertent initiation of the ADS.
- (iii) Since the RHR is initiated by an operator action, its initiation time is set at 30 minutes from the event occurrence.
- (iv) One out of three RHRs is credited.
- (v) The initial core flow is set at 90%, as a representative case, because differences of assumed initial core flow have only a slight effect on the comparison of the results against the acceptance criteria.
- (vi) The operating mode of the RFC (Class 3) is assumed to be manual (frozen).
- (vii) The EHC (Class 3) is assumed to be working. This is conservative, because freezing the EHC decreases the reactor pressure faster, and so the reactor pressure reaches the MSIV closure setpoint before the D/W pressure reaches the high D/W pressure scram setpoint. Therefore the reactor achieves shutdown conditions earlier, which results in less severe

pressure and temperature of the S/P than in the case that the EHC is assumed to be working.

- (viii) The FDWC (Class 3) is assumed to be working because the effect on the reactor power and pressure of freezing the FDWC is negligible.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is an infrequent fault, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

AC-D3: Dose to workers should be less than 200 mSv.

AC-D4: Dose to members of the public should be less than 10 mSv.

(c) Fault Progression

Inadvertent opening of all of the ADS SRVs allows steam to be discharged into the suppression pool and the suppression pool temperature and pressure is increased. The sudden increase in the rate of steam flow leaving the reactor vessel causes a depressurisation. Though the reactor scram is initiated by the high D/W pressure and shutdown is achieved, the pressure and temperature of the S/P keep increasing because steam from the reactor keeps going into the S/P after the shutdown. However one RHR can cool the S/P and the reactor core as demonstrated in the analysis for a main steam line break inside primary containment presented in Section 24.8.3.1.

(d) Analysis Results

The analysis results of the Inadvertent opening of all ADS event are shown in Table 24.9-12 and Figure 24.9.3-1.

The analysis results are compared with the acceptance criteria described above as shown below:

- In the case of an OLMCPR value of 1.28 or more, the MCPR is greater than the safety limit MCPR value (1.06), so that boiling transition does not occur after the event. Therefore the maximum fuel cladding temperature is less than the acceptance criterion value of 1200 °C and the oxidation of the fuel cladding is less than the acceptance criterion value of 15 %. (AC-F5 and AC-F4 met with significant margin)

- The pressure and temperature behaviour of the S/P after the event is bounded by the corresponding behaviour for the main steam line break inside primary containment (see Section 24.8.3). Thus, the peak pressure on the primary containment boundary does not exceed the acceptance criterion value of 0.310 MPa [gauge] (AC-C1 met) and the peak suppression pool temperature does not exceed the design temperature limit of 104 °C.
- In the same way as pressure on the primary containment, the impact of radiation dose to the public and workers is bounded by the main steam line break inside primary containment and therefore the acceptance criteria relating to radiation exposure are met. (AC-D4 and AC-D3 met with significant margin)

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the acceptance criteria are met for this event.

Although a direct CCF of Class 1 SSCs event is treated as an infrequent DB event, the acceptance criteria are shown to be met using Class 2 SSCs to provide the relevant HLSFs. Normally, the NSEDPs require that the principal protection against DB faults should be Class 1. However, [Ref-34] provides evidence that, in the particular case that the initiating event for an infrequent DB fault involves the CCF of Class 1 SSCs, it is ALARP to rely on the Class 2 diverse provision of the corresponding HLSFs.

Table 24.9-12: Results Summary for Inadvertent Opening of All ADS

Item	Value	time
Maximum Neutron Flux (%)	100.0	0.0 s
Maximum Average Heat Flux (%)	100.9	0.2 s
Maximum Vessel Bottom Pressure (MPa [gauge])	7.28	0.0 s
ΔMCPR	0.08	82.4 s

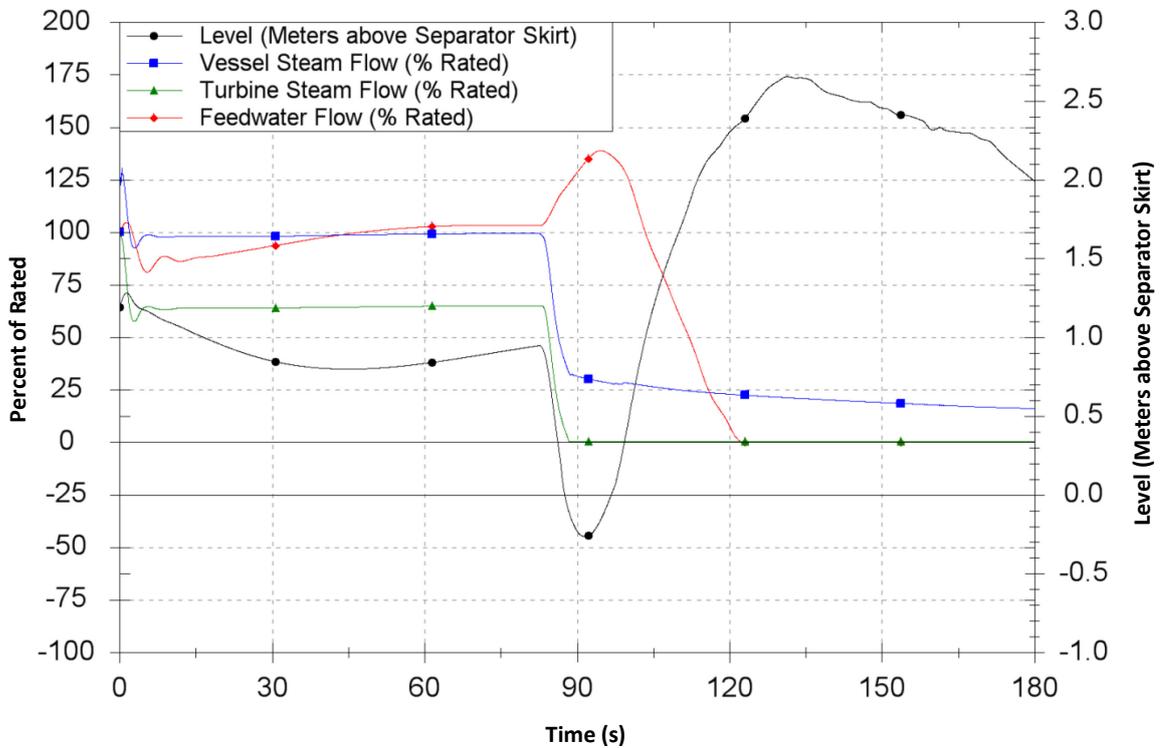
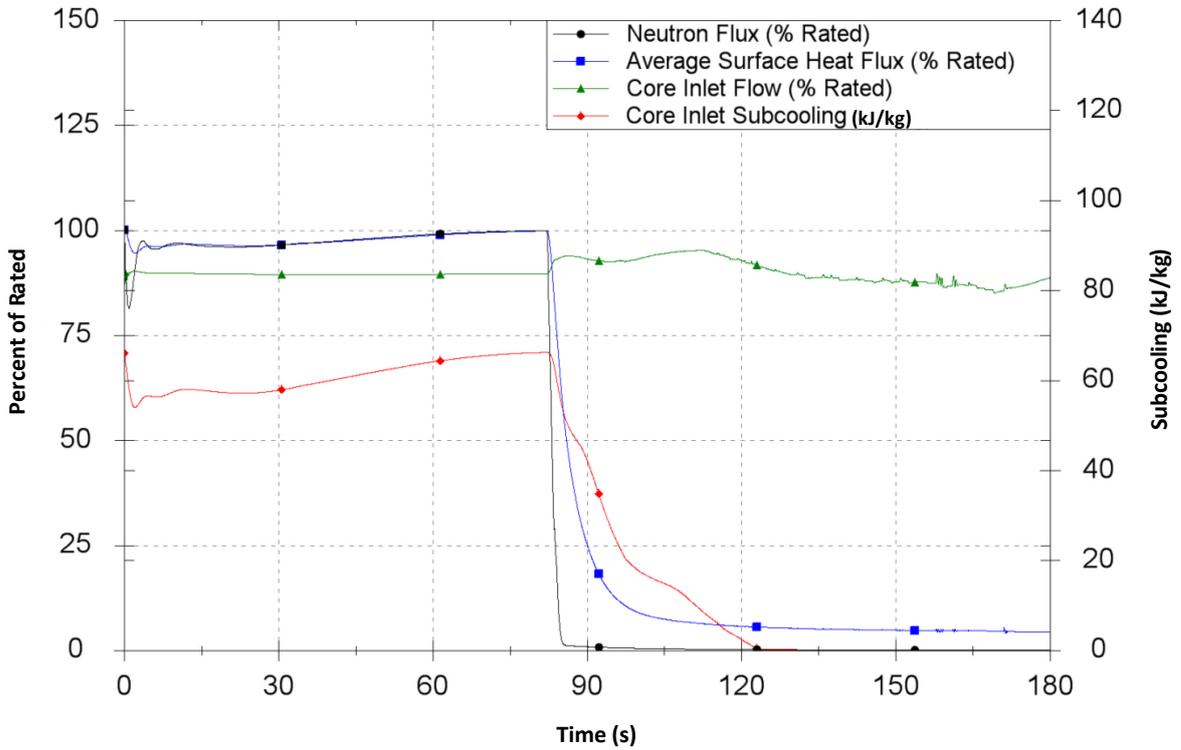


Figure 24.9.3-1: Inadvertent Opening of All ADS

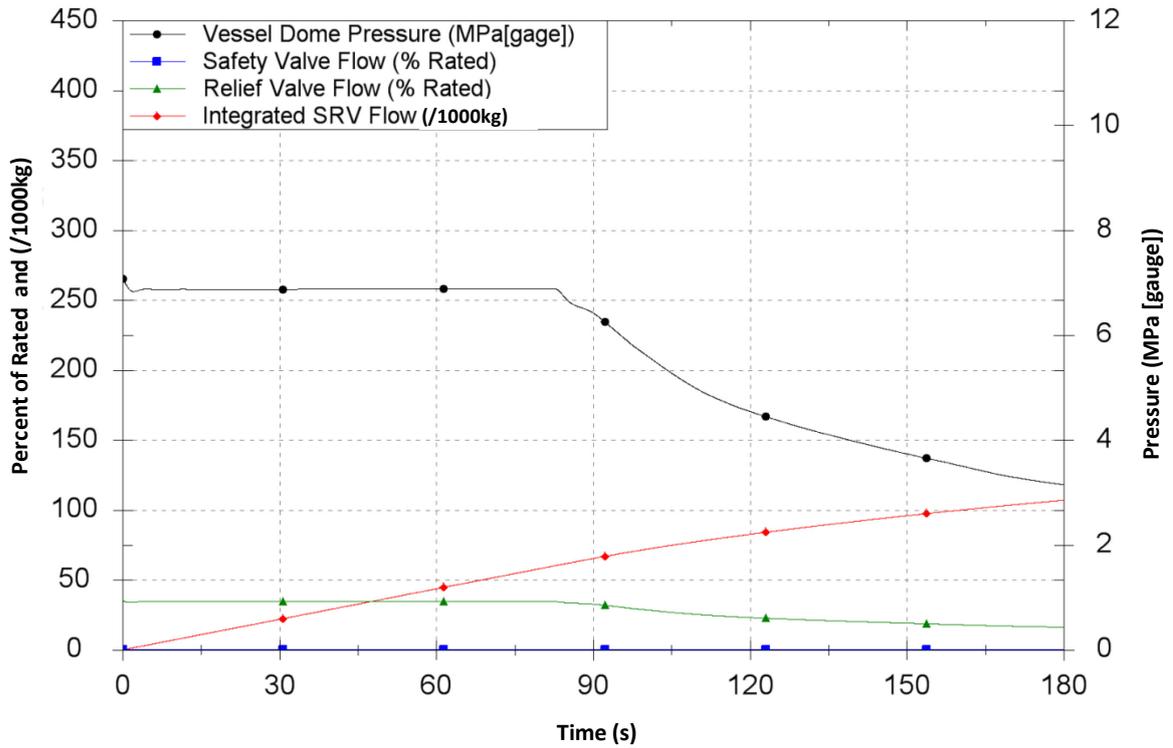


Figure 24.9.3-1: Inadvertent Opening of All ADS (Continued)

24.9.3.2 All Rod Insertion Fault

Fault Schedule Ref: 11.1

(1) Description of Fault

During power operation, FMCRD run-in is initiated by malfunction of RCIS and all the control rods are inserted simultaneously starting from the same position with the same speed. The fault is assumed to be a frequent fault.

(2) Plant normal response

The main protection against the fault is described below:

- (i) If a FMCRD run-in signal is generated by RCIS, a run-back requirement signal is given to decelerate all RIPS to the minimum speed, controlling the excessive local power peaking.
- (ii) If the separation detection is not triggered following a scram or Alternative Rod Insertion (ARI) demand (indicating the failure of hydraulic insertion), in order to avoid large axial local power peaking during the FMCRD control rod run-in, the control rods are divided into 4 groups and inserted sequentially by the electric drive with appropriate time intervals.
- (iii) Scram is initiated by the Axial-Peaking Power Range Monitor (A-PPRM) difference being greater than 140%.

(3) Analysis of Event**(a) Analysis Assumptions**

The following conditions are used in the analysis:

- (i) In order to increase radial peaking, the initial control rod pattern consists of the design control rod pattern and additional fully inserted control rods.
- (ii) The initial power is set at the rated power, with the reactor pressure at 7.07 MPa [gauge].
- (iii) A control rod scram is initiated by the A-PPRM when the difference between upper and lower neutron flux reaches 140%.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is a frequent fault, they are:

- AC-F1: The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.

AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.

AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.

(c) Fault Progression

During the power operation, FMCRD run-in is initiated by malfunction of RCIS with consideration of CCF, and all the control rods are inserted simultaneously starting from the same position with the same speed. The slow insertion by FMCRD run-in increases the distortion of axial power distribution since RIPS run-back and grouped run-in do not work due to CCF. A control rod scram is initiated by the A-PPRM difference being very large at 140%, and then the fault is terminated by the scram. The transient results in a heat flux increase of approximately 9%. The change (reduction) in critical power ratio (Δ CPR) for this event is 0.14. The reactor pressure does not increase significantly as the reactor power does not increase significantly during the fault.

(d) Analysis Results

The summary of the analysis results are as follows:

- In the case of an OLMCPR value of 1.28 or more, the MCPR is greater than 1.14, and so remains above the safety limit MCPR (1.06) (AC-F1 met).
- The transient results in a heat flux increase of approximately 9%, and therefore does not exceed the TOP or MOP acceptance criteria (AC-F2 met).
- The reactor pressure does not increase significantly as the reactor power does not increase significantly during the fault, and therefore does not exceed the acceptance criterion of 9.48 MPa [gauge] (AC-R1 met).

The acceptance criteria described above are met.

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the DBA acceptance criteria are met for this event. As a result, there are no radiological release and no exposure of workers or the public.

There are a number of Class 3 SSCs providing the HLSFs claimed in this analysis in addition to the Class 1 SSCs in Table 24.6-1. These provide defence in depth and contribute to the claim that the risks from this event are ALARP.

24.10 Analysis Results and Fault-based View – Reactor Faults Other Than at Full Power

Depending on the operational mode of the reactor, the full range of protection systems may not be available. Further, in some operational modes, the transient behaviour of the reactor is different from that at full power. These considerations mean that it cannot be assumed that all faults are bounded by the at-power case.

In this section, two types of faults are considered:

- Faults occurring in partial power operation – see Section 24.10.1
- Faults occurring in shutdown modes – see Section 24.10.2

24.10.1 Faults Occurring in Partial Power Operation

The identified bounding faults during partial power operation shown in Section 24.4.5 are as below.

- Generator load rejection (without power load unbalance relay) (Fault Schedule Ref: 12.1)
- Generator load rejection on scram bypass power (Fault Schedule Ref: 12.2)
- Trip of all RIPs on scram bypass power (Fault Schedule Ref: 12.3)

The details of the results of the analysis for these events are shown in the Topic Report on Design Basis Analysis [Ref-5].

Analysis of Generator load rejection on scram bypass power is described as the representative case among the above events. This is assumed to be a frequent fault as it is caused by the failure of a Class 3 system.

The HLSFs at partial power are provided by the same SSCs as for full power operation and are shown in Table 24.6-1. Provisionally, it is assumed that scram is initiated by high pressure in the RPV or by high neutron flux.

Parameters relating to the protection against this fault are shown in Table 24.10-2 and Table 24.10-3.

Analysis conditions for this fault at partial power are shown in Table 24.10-1.

Table 24.10-1: Analysis Conditions

Item	Analysis Conditions	Note
Reactor thermal power	35% of the rated power	<ul style="list-style-type: none"> • Rated power: 3926 MW • 35% is the maximum reactor power at which the scram is bypassed.
Fuel type	10 × 10 Fuel (GE 14)	-
Fuel rod peak linear heat generation rate	15.4 kW/m	-

Table 24.10-1: Analysis Conditions (Continued)

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

Item	Analysis Conditions	Note
Core flow	96% of the rated core flow	<ul style="list-style-type: none">Rated core flow: 52200 t/h96% is the maximum core flow at 35% of the reactor power.
Reactor Dome pressure	Reactor dome pressure at 35% of the reactor power	Dome pressure at the rated reactor power : 7.07 MPa [gauge]
Steam flow	Steam flow at 35% of the reactor power	Rated steam flow: 7640 t/h
Water level	Normal operating water level	-

Limits and Conditions for Operation

No LCOs are identified in addition to those in Section 24.6.

24.10.1.1 Generator Load Rejection on Scram Bypass Power

Fault Schedule Ref: 12.1

(1) Description of Fault

In a state in which the reactor power is less than 35% of rated power, the function of scram on main steam valve closure and TCVs rapid closure is bypassed in the RPS, and after a generator load rejection the reactor pressure is controlled by the turbine bypass valve.

The turbine bypass valve function is not categorised as an A1 function, and so this function cannot be credited in Design Basis analysis. As the result, the reactor pressure is increased and scram occurs on high reactor pressure scram or on high neutron flux.

(2) Plant normal response

In practice, PLURY which triggers rapid TCV closure isn't initiated when the generator power is below 40%. Instead EHC (Class 3) controls TCVs and TBVs in response to the increase of turbine speed signal. Thereby reactor pressure remains stable and thus the plant reaches a stable state.

(3) Analysis of Event**(a) Analysis Assumptions**

The analysis conditions for the analysis are listed in (i) to (xii) below. The details of the analysis conditions are described in Attachment-I.3.1 in the Topic Report on Design Basis Analysis [Ref-5].

- (i) The initial conditions of the analysis are shown in Table 24.10-1.
- (ii) The closure characteristics of the TCVs are assumed such that the valves operate in the full arc (FA) mode and have a full stroke closure time, from fully open to fully closed, of 0.15 seconds. (In the analysis, less than 0.15 seconds is required to close the valve because the valve is not fully open at the beginning of the transient.)
- (iii) The TBVs are not credited to show that the event is stabilised by taking credit for A1 functions only.
- (iv) The RPT is not credited to show that the event is stabilised by taking credit for A1 functions only.
- (v) The initial reactor power is set at 35% of rated power.
- (vi) In practice PLURY is not initiated and the TCVs do not rapidly close. However, for the analysis rapid TCV closure is assumed to analyse the event more conservatively in terms of the calculated pressure rise.
- (vii) Scram on rapid TCV closure is assumed to be bypassed because the power is 35% at the

time of the TCV closure.

- (viii) The initial core flow is set at 96% which is the maximum core flow at the assumed reactor power of 35%. The core void fraction at 96% core flow is smaller than that at 42% core flow. This provides less void reactivity on rapid TCV closure and takes more time to reach the scram setpoint of high neutron flux or high reactor pressure, which results in higher thermal power. From this point of view, the initial core flow is conservatively set at 96%.
- (ix) The operating mode of the RFC (Class 3) is assumed to be manual (frozen). (As this is frozen, it does not constitute a HBSC).
- (x) The EHC (Class 3) is assumed to be working because the TCVs are closed at the event initiation and TBVs are not credited.
- (xi) The FDWC (Class 3) is assumed to be working, as a representative case, because the effect on the peak reactor power and pressure of freezing the FDWC is negligible.
- (xii) One division of each SSC in Table 24.6-1 is available

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, which is a frequent fault, they are:

AC-F1: The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling.

AC-F2: Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the TOP or the MOP limits.

AC-R1: Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure.

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

(c) Fault Progression

Rapid TCV closure increases the reactor pressure and this pressure increase reduces voids in the core. This provides positive void reactivity and so the reactor power increases. Since the reactor power is less than 35% at the time of rapid TCV closure, rapid TCV closure scram is bypassed and the reactor pressure and power keeps increasing. Ultimately, the reactor pressure reaches the scram setpoint and the event is stabilised.

(d) Analysis Results

The analysis results of the Load Rejection without Bypass at 35% rated power and 96% rated core flow are shown in Table 24.10-4 and Figure 24.10.1-1.

The analysis results are compared with the acceptance criteria described above as below.

- When the initial MCPR is greater than 2.02, the MCPR is greater than 1.06, and so remains above the safety limit MCPR value (1.06). (AC-F1 met with significant margin)
- The peak surface heat flux of the fuel cladding is approx. 56.7%, and so does not exceed the acceptance criterion 138%. (AC-F2 met with significant margin)
- The peak pressure on the reactor coolant pressure boundary is 8.41 MPa [gauge], and so it does not exceed the acceptance criterion value of 9.48 MPa [gauge]. (AC-R1 met with some margin)
- Pressure on the primary containment boundary does not exceed the maximum allowable working pressure. (AC-C1 met with significant margin)

(4) Discussion and Conclusions

The results of the analysis of this fault show that all the acceptance criteria are met with a large margin. In addition, only Class 1 protection is claimed in the analysis, whereas there are additional Class 3 (EHC) controls TCVs and TBVs properly to keep reactor pressure stable. The margin on acceptance criteria and the availability of additional control function make the risk from this fault very low. There are no additional reasonably practicable means of further reducing the risk and the risk is deemed to be ALARP.

Table 24.10-2: Analysis Setpoints of Safety System

Item	Analysis Conditions	Note
High reactor pressure scram	7.62 MPa [gauge]	-
High neutron flux scram in terms of neutron flux	125%	-
Rapid TCV closure scram	Rapid TCV closure	Rapid TCV closure scram is initiated on the condition that reactor power is higher than 35%.

*The 2 out of 4 logic is applied for Class 1 safety systems, as described in Chapter 14. Therefore the system maintains the safety functions even when considering single failure and maintenance.

Table 24.10-3: Plant Specifications Related to Other Systems

Item	Analysis Conditions	Note
Fast Turbine steam control valve closure time	0.15 s	<ul style="list-style-type: none"> • This value is the closure time from fully open to fully closed. • Though PLURY is not initiated and TCVs do not close rapidly at 35% of reactor power, PLURY is assumed to work to close the TCVs rapidly for the analysis to produce more conservative analysis results.
Scram insertion time	1.71 s at 60% of full stroke 3.70 s at 100% of full stroke	The setpoints of the scram insertion time at the rated pressure are 1.44 seconds or less at 60% insertion of full stroke and 2.80 seconds or less at 100% insertion of full stroke. However, in analysing abnormal operational transients, 1.71 seconds at 60% insertion and 3.70 seconds at 100% insertion are used. The dependence of the control rod drive system on the reactor pressure was taken into consideration to determine these values.
Safety Relief Valve setpoints (Safety function)	1st stage : 8.17 MPa [gauge] 2 valves 2nd stage : 8.24 MPa [gauge] 4 valves 3rd stage : 8.31 MPa [gauge] 4 valves 4th stage : 8.38 MPa [gauge] 3 valves 5th stage : 8.45 MPa [gauge] 3 valves	Analysis conditions are 3% larger than nominal setpoints.

Table 24.10-4: Results Summary for Load Rejection without Bypass at 35 rated power and 96 rated core flow

Item	Value	Time
Maximum Neutron Flux (%)	73.6	5.8 s
Maximum Average Heat Flux (%)	56.7	6.3 s
Maximum Vessel Bottom Pressure (MPa [gauge])	8.41	8.8 s
Δ MCPR	0.96	6.7 s

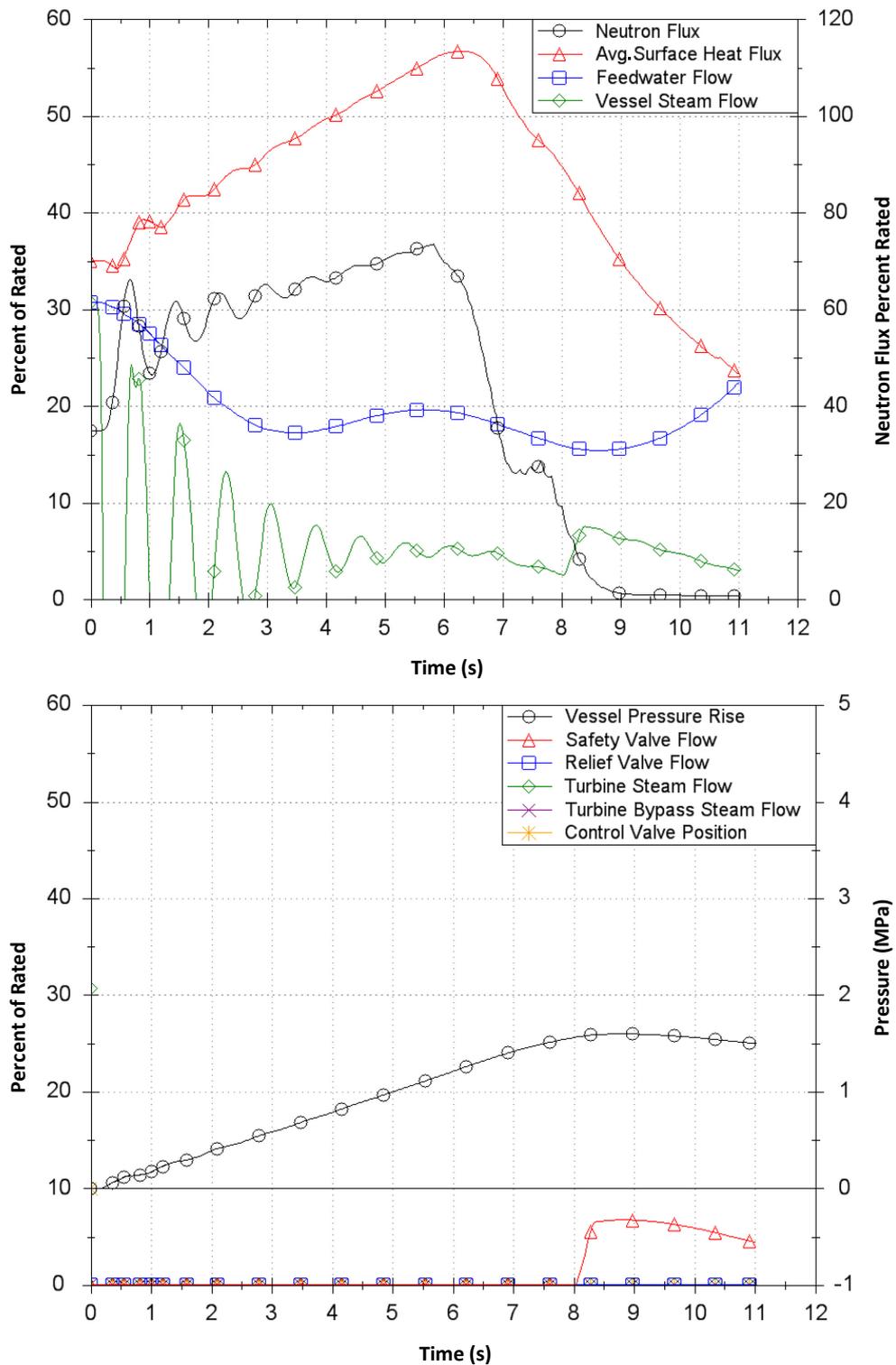


Figure 24.10.1-1: Load Rejection without Bypass at 35 rated power and 96 rated core flow

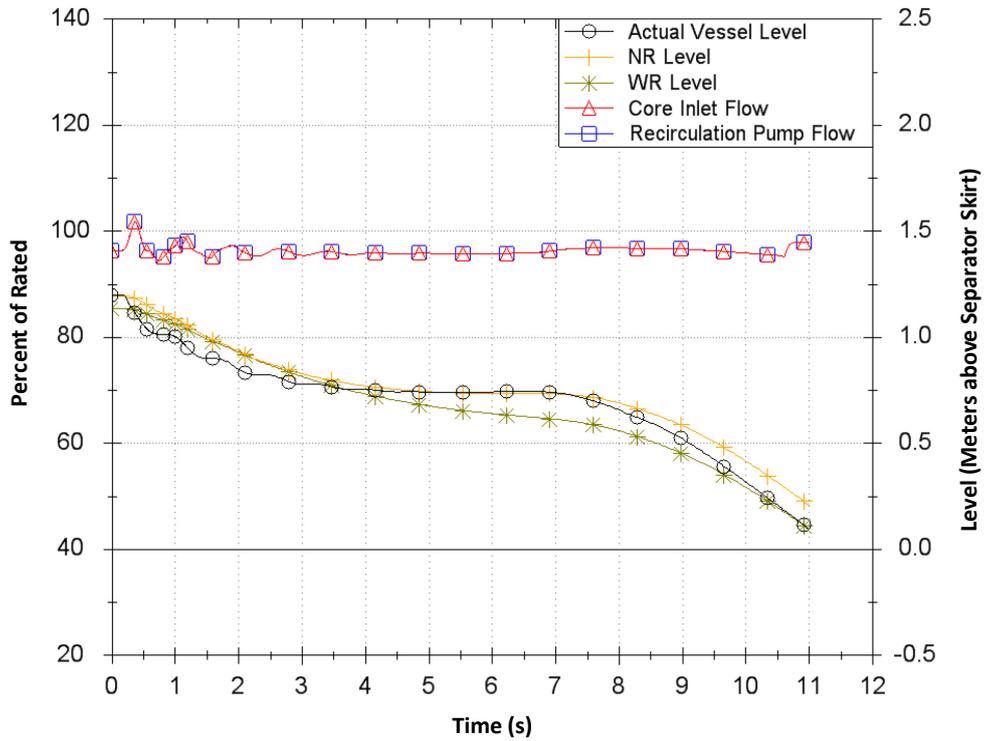


Figure 24.10.1-1: Load Rejection without Bypass at 35 rated power and 96 rated core flow (Continued)

24.10.2 Reactor Faults in Shutdown Modes

Loss of heat removal functions are the principal failures to be considered during shutdown modes. These fall into two groups:

- Loss of decay heat removal – see Section 24.10.2.1
- Loss of reactor coolant – see Section 24.10.2.2

This section presents transient analysis results for representative design basis faults in reactor shutdown modes (Operating state C) to confirm adequacy of the safety design and suitability and sufficiency of the safety measures regarding the ability to meet DB targets in the NSEDPs. Each operating state considered (C-1 to C-5) is explained below. The corresponding Plant Operating States (POS) used in Chapter 25 are also shown.

Figure 24.10.2-1 shows the plant operating states in reactor shutdown modes for the UK ABWR, and the configuration of the RPV head and the reactor well for each state are shown in Figure 24.10.2-2, through Figure 24.10.2-6.

(1) Operating State C-1: Transition to reactor cold shutdown (POS S)

This operating state is implemented for the first day after the vacuum break of the main condensers. It is characterised by the highest decay heat and availability of all of the RHRs together with the ECCS (except for the turbine driven RCIC). The water level is the same as that in normal operation. Decay heat of the reactor core is removed by the shutdown cooling mode of one division of the RHR.

(2) Operating State C-2: Transition to reactor disassembled and reactor well gate open (POS A)

This operating state is implemented for a period from the end of operating state C-1 to completion of reactor well flooding. This operating state takes place from the second to the third day where the reactor is disassembled (i.e. by opening the RPV and PCV top heads) and water level increases from the RPV flange level to the normal water level of the reactor well. Due to the large decay heat even in this period, this decay heat is still removed from the reactor core by the shutdown cooling mode of one division of the RHR.

Note that the Shutdown Level 1 PSA assumes the RPV head on in order to assess more onerous accident sequences than those with the RPV head off.

(3) Operating State C-3: Full water level in reactor well and gate open (POS B)

This operating state is implemented for a period from “opening the reactor well gate” to “closing the reactor well gate”. As the water inventory is sufficiently large, reactor coolant is not likely to heat up

significantly in this time period even if decay heat removal is lost. This operating state is subdivided into C-3-1, C-3-2 and C-3-3 corresponding to the available sets of mitigation systems available or in maintenance according to the assumed maintenance schedule.

(4) Operating State C-4: Transition to closed condition of PCV/RPV top heads (POS C)

This operating state is implemented for a period from “closing the reactor well gate” through “starting drain off of reactor well” to “completing the RPV leak test”. Inspection and maintenance of equipment may continue in this period, and this operating state is subdivided into C-4-1 and C-4-2 corresponding to the mitigation systems available or in maintenance according to the assumed maintenance schedule. Though the water level decreases from the normal water level of the reactor well to the RPV flange level, it is higher than that at the normal operation and the decay heat is much less than that just after reactor shutdown. Therefore, plant behaviour in a faulted condition is milder than that in operating state C-2.

Note that the Shutdown Level 1 PSA assumes the RPV head on in order to assess more onerous accident sequences than those with the RPV head off.

(5) Operating State C-5: Preparation of plant startup (POS D)

This operating state is implemented a period from “completing the RPV leak test” through “PCV assemble and leak test” to “starting CR withdrawal for startup”. During this period, inspection and maintenance of equipment for heat removal and makeup have been completed, therefore all ECCS except the turbine driven RCIC, and most of other mitigation systems are in standby. The decay heat is much less than that of just after reactor shutdown. Therefore, plant behaviour in a faulted condition is milder than that in operating state C-1.

(6) Operating State C-6: Full core off-loaded to the SFP (POS E)

Full core off-load is defined as the period of the condition for full core offload from reactor. The refuelling outage with full core off load is not performed in every operation cycle. In long term outage in order to some focussed inspection or after forced shutdown, full core may be removed from core and stored in the SFP. It is assumed that the thermal load of the isolated SFP is bounded in this plant configuration.

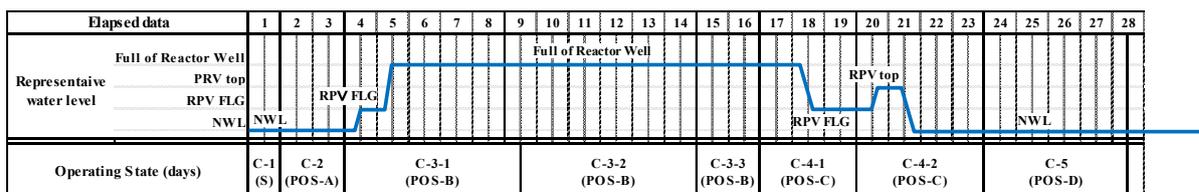


Figure 24.10.2-1: Typical Outage Schedule in Shutdown Modes for UK ABWR

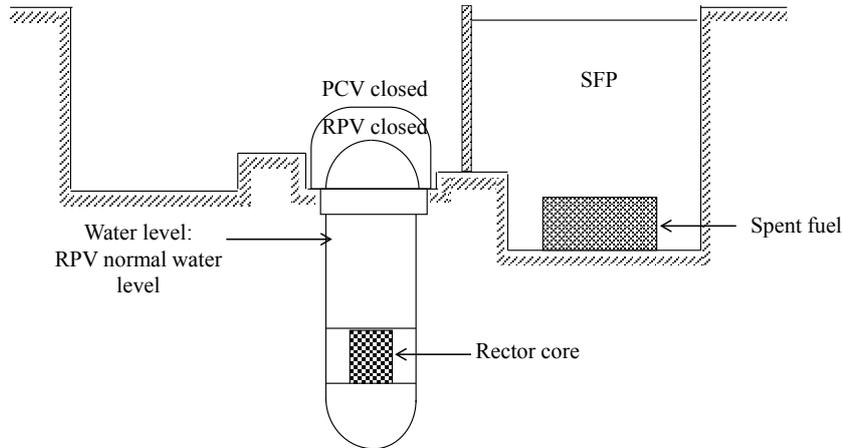


Figure 24.10.2-2: Operating State C-1 and C-5 (RPV top head on and Reactor well gate closed)

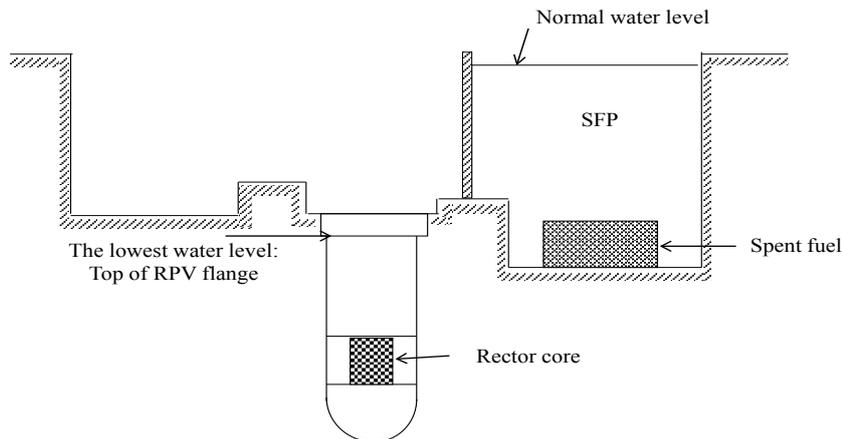


Figure 24.10.2-3: Operating State C-2 (RPV top head off and Reactor well gate closed)

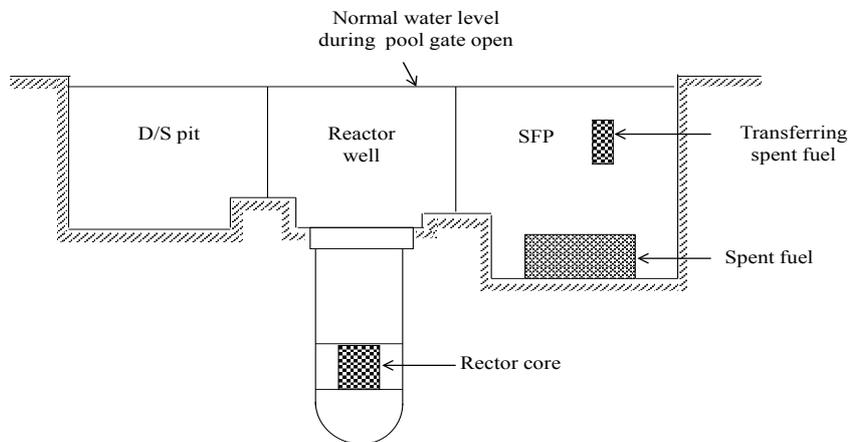
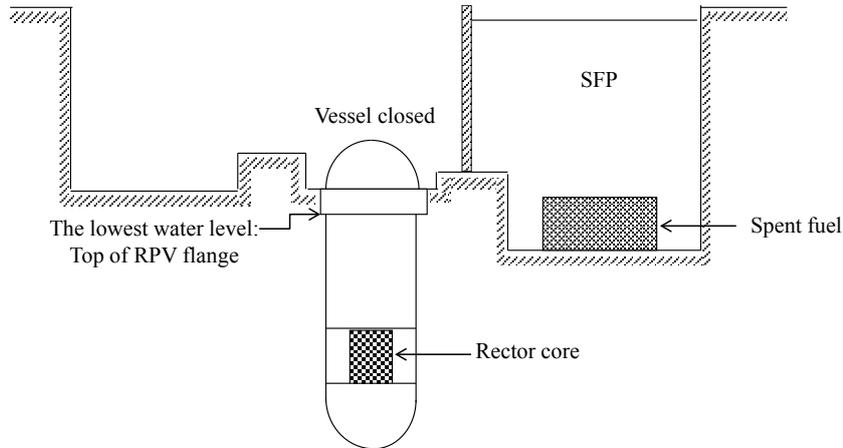
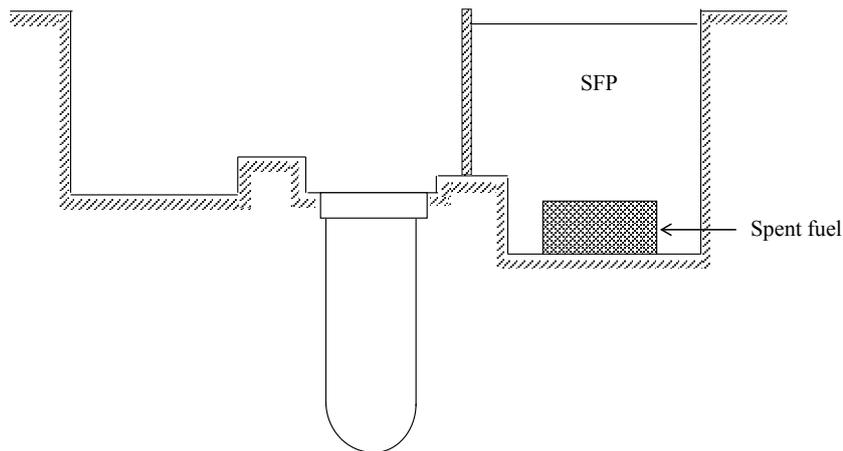


Figure 24.10.2-4: Operating State C-3 (Reactor well gate open)



**Figure 24.10.2-5: Operating State C-4
(RPV top head on, PCV head off, and Reactor well gate closed)**



**Figure 24.10.2-6: Operating State C-6
(No fuel in RPV, SFP isolated, SFP gate closed)**

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

In shutdown modes, the main fault to be considered is loss of heat removal since criticality is already controlled. Loss of heat removal may lead to fuel cladding damage. In some modes, because the reactor coolant circuit and primary containment are not available (RPV vessel head removed and PCV head removed), fuel cladding is the only barrier to release of activity. All fuel operations occur under water, so the SFP and reactor well water provide some protection against release.

In addition to the above, as the plant is in a shutdown mode, the hatches and the personnel airlocks in the PCV are assumed to be in the open state.

As the boundary of the PCV is therefore not intact, if a fault occurs, it could lead to consequential internal flooding in the R/B because water or steam released from the reactor and SFP could inflow to the R/B via the open hatches and airlocks. The internal flooding could lead to consequential effect on the safety divisions.

Moreover, depending on the fault scenarios, re-closing the airlocks and hatches is important to ensure the PCV boundary integrity and to limit the loss of water inventory in the PCV.

Table 24.10-5 shows the SSCs available to provide the required HLSFs during shutdown.

Due to maintenance activities during shutdown, not all divisions of each SSC in Table 24.10-5 are available in all modes. Thus, the maintenance schedule is taken into consideration in the transient analysis of these modes.

Analysis conditions for reactor faults in shutdown modes are shown in Table 24.10-6.

NOT PROTECTIVELY MARKED

Table 24.10-5: Provision of HLSFs in Shutdown Modes

HLSF	SSC	PCSR Ref	Notes
1-3 Emergency shutdown of the reactor	CRD (Class 1)	11.5.2, 12.4.3.1	Control rods are inserted rapidly in the event of control rod withdrawal error.
1-4 Functions to maintain sub-criticality	CRD (Class 1)	11.5.2, 12.4.3.1	CRD maintains sub-criticality in the reactor core during shutdown.
1-9 Functions to maintain sub-criticality of spent fuel outside the reactor coolant system	SFP racks (Class 1)	19.8.2.1	SFP racks maintain sub-criticality of storage fuel in all operating modes.
2-1 Functions to cool reactor core	HPCF (Class 1)	13.4	Power for HPCF is provided by EDG.
	LPFL (Class 1)	13.4	LPFL is a function of RHR. Power for LPFL is provided by EDG.
	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to control SSCs related to HPCF and LPFL.
2-2 Function of alternative fuel cooling	FLSS (Class 2)	16.7.3.1	FLSS provides makeup water into the reactor core. Power for FLSS is provided by BBG.
	RDCF (Class 2)	16.7.3.3	RDCF depressurises the RPV by the operator for the water injection on the condition of RPV head closed (Operating state C-1, C-4 and C-5)
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to FLSS and RDCF.
	FLSR (Class 3)	16.7.3.2	FLSR provides makeup in the event of failure of FLSS.
	Fire Protection System (Class 3)	16.6.3	Fire Protection System provides makeup water in the event of failure of FLSS.
2-4 Functions to cool spent fuel outside the reactor coolant system	FPC (Class 1)	19.9	FPC is a two division Class 1 system providing cooling to SFP during all normal operating modes, Heat is rejected to RCW and RSW
	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to control SSCs related to FPC.
2-5 Functions to make up water for spent fuel pool	FLSS (Class 2)	16.7.3.1	FLSS provides makeup water into the SFP in the event of loss of decay heat removal, and LOCA in operating state C-3.
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to FLSS and RDCF.

Table 24.10-5: Provision of HLSFs in Shutdown Modes (Continued)

HLSF	SSC	PCSR Ref	Notes
3-1 Functions to remove residual heat after shutdown	RHR (Class 1)	12.3.5.4	RHR is a three division Class 1 system providing cooling to the reactor during shutdown modes. Heat is rejected to RCW and RSW. Power for RHR is provided by EDGs.
	SRV (Class 1)	12.3.5.2	SRVs depressurise the RPV by the operator for long term heat removal in the event of loss of decay heat removal on the condition of RPV head closed (Operating state C-1, C-4 and C-5).
	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to control SSCs related to RHR and SRV.
3-2 Function of alternative containment cooling and decay heat removal	AC FCVS (Class 2)	13.3.3.4	AC or FCVS are used for Containment Venting to deliver long term PCV heat removal and overpressure protection in the event of loss of decay heat removal on the condition of PCV head closed (Operating state C-1 and C-5)
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to AC and FCVS.
4-7 Function to confine radioactive materials, shield radiation, and reduce radioactive release	PCIS (Class 1)	13.3.3.2	Closure of isolation valves prevents reactor coolant outflow to outside the PCV in the event of LOCA outside PCV.
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system.
	HWBS (Class2)	14.6.3	HWBS provides the functions to generate actuation signals for the second line of safety systems.
5-2 Supporting functions especially important to safety	Class 1 EPS (Class 1)	15.3	Class 1 EPS supplies power to Class 1 SSCs. EDG supports SSCs related to HPCF, LPFL and RHR.
	RCW/RSW (Class 1)	16.3.2	RCW/RSW are essential systems for supporting HPCF, RHR and Class 1 HVAC operations.
	UHS (Class 1)	16.3.1	UHS provides sufficient cooling water to the RSW.

Table 24.10-5: Provision of HLSFs in Shutdown Modes (Continued)

HLSF	SSC	PCSR Ref	Notes
5-3 Function of alternative supporting system	B/B Class 2 EPS (Class 2)	15.4.6, 15.4.8.4	B/B Class 2 EPS including B/B Class2 DC power supply system supplies power to the second line of safety systems. BBG supports SSCs related to alternative fuel cooling and alternative long term heat removal.
	EECW (Class 2)	16.3.6	EECW supplies recirculation cooling water to BBG auxiliaries.
5-5 Function to shutdown safely from outside the control room	RSS (Class 1)	14.6.2.2	RSS supports manual initiation of HPCF, SRV and RHR in the event of CCF of SSLC.
5-6 Functions to handle fuel safety	FHM (Class 1)	19.6	Hoist of the FHM stops to prevent drop of lifting body in case of LOOP.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 1 HVAC (Class 1)	16.5	Class 1 HVAC ensures the adequate environmental parameters for Class 1 SSCs are maintained.
	HECW (Class 1)	16.3.5.1	HECW provides chilled water for Class 1 HVAC.
	Class 2 (A2) HVAC (Class 2)	16.5	Class 2 (A2) HVAC ensures the adequate environmental parameters for SSCs related to SLC are maintained.
	HBCW (Class 2)	16.3.5.3	HBCW provides chilled water for Class 2 (A2) HVAC.

Table 24.10-6: Analysis Conditions for Reactor Faults in Shutdown Modes

Items	Analysis conditions
	RPV
Fuel type	10 × 10 Fuel (GE 14)
Fuel operation cycle condition	17 month operation and 30 days outage
Elapsed time from reactor shutdown	4 days
Decay heat	21.9 MW
Initial water level	SFP normal water level
Initial water temperature	52 °C
FLSS flow (rated value for RPV injection)	1100 m ³ /h
FLSS flow (rated value for SFP injection)	120 m ³ /h
Initiation signal of water injection for RPV	RPV low water level alarm (Level 3)
Initiation signal of water injection for SFP	SFP low water level alarm
RPV activity level	DB Primary Source Term as defined in Chapter 20 and 23
SFP activity level	SFP DB Source Term as defined in Chapter 20 and 23

Limits and Conditions for Operation

The future licensee shall ensure that, during normal shutdown operations, the following plant conditions are maintained:

- The RPV water level shall be above the low water alarm level
- The SFP water level shall be above the low water alarm level

The future licensee shall ensure that, during normal shutdown operations, no more than one division of the following systems and their support systems in the same division shall be subject to testing or maintenance:

- RHR
- FPC
- HPCF
- SSLC
- Class 1 EPS
- EDG
- RCW
- RSW

- UHS
- Class 1 HVAC
- HECW
- FLSS
- HWBS
- B/B Class 2 EPS
- BBG
- EECW
- Class 2 (A2) HVAC
- HBCW

The future licensee shall ensure that, during normal shutdown operations, the following SSC s are operational:

- CRD in case that the fuel is loaded in the core
- PCIS
- FLSR
- Fire Protection System in case that one division of FLSS and its support systems are in maintenance

The future licensee shall ensure that, during normal shutdown operations on condition of the PCV head is closed, no more than one division of the following systems and their support systems in the same division shall be subject to testing or maintenance:

- AC and FCVS treated as one system

The future licensee shall ensure that, during normal shutdown operations on condition of the RPV head is closed, the following SSC is operational:

- SRV
- RDCF

The future licensee shall ensure that, in all operational modes, the reactor and SFP activities are below the DB Source Term as defined in Chapter 20.

24.10.2.1 Loss of Decay Heat Removal in Reactor Shutdown Modes

All initiating events which are categorised as loss of decay heat removal faults in reactor shutdown modes are summarised as follows:

- Loss of operating RHR with loss of the same division of ECCS (Fault Schedule Ref: 13.3)
- Loss of operating RHR due to CCF of Class 1 controller (Fault Schedule Ref: 13.4)
- Short term station blackout (2 hours duration) (Fault Schedule Ref: 13.6.1)
- Medium term station blackout (24 hours duration) (Fault Schedule Ref: 13.6.2)
- Inadvertent start-up A1 (RHR, HPCF) injection system (Fault Schedule Ref: 11.6)
- Inadvertent start-up A2 (FLSS) injection system (Fault Schedule Ref: 11.7)
- M/C power supply failure on electrical CCF (Fault Schedule Ref: 11.8)
- Loss of all RCW (Fault Schedule Ref: 11.10)
- Loss of all RSW (Fault Schedule Ref: 11.11)
- Loss of all Class 1 HVAC (Fault Schedule Ref: 11.12)

The representative event in the loss of decay heat removal fault group is “Loss of operating RHR with loss of the same division of ECCS” in “Operating state C-3”. The fault loss of decay heat removal in shutdown modes is designated as an infrequent fault.

24.10.2.1.1 Loss of operating RHR with loss of the same division of ECCS

Fault Schedule Ref: 13.3

(1) Description of Fault

During shutdown, one division of the RHR operating in reactor shutdown cooling mode is used to cool the reactor core, and one division of the FPC is used to cool the SFP. In operating state C-3, the reactor well gate is open and the reactor well and SFP form one body of water.

Loss of Class 1 AC due to failure of a switchboard in a Class 1 AC bus could cause loss of the operating RHR and its support systems of standby HPCF, EDG and operating FPC in the same division. This case results in an increase of water temperature and decrease of water level after boil-off.

If reactor and SFP cooling are lost, boiling of the reactor well water cannot be prevented. The reactor well and SFP boiling could eventually lead to uncovering of the reactor core and spent fuel in the SFP leading to fuel damage and a large release of activity. However, even in the case of loss of decay heat removal, there are three diverse and independent means of introducing water to the reactor and SFP:

- FLSS (Class 2) - Operator initiation is claimed in the fault assessment and is covered by HBSC HF FLSS 2-3.1 and HBSC HF FLSS 2-3.2 (see Table A-2 of this chapter, and details for Chapter 27 Appendix A)
- FLSR or Fire Protection System (Class 3) – In the event that FLSS is unavailable (considered CCF event in limited operating states or BDB event), operator initiation of FLSR or Fire Protection System provides the necessary makeup. This is covered by HBSC HF FLSR 2-3.1 (see Table A-2 of this chapter, and details for Chapter 27 Appendix A)

(2) Plant Normal Response

In a loss of decay heat removal event, the operator initiates the standby RHR to remove decay heat and HPCF or LPFL to make up water level. Here, either one of the three independent RHR divisions is lined up in the shutdown cooling mode. In addition, even if one division of the FPC is in operation in a pre-fault condition, the operator initiates the standby FPC to remove decay heat in the SFP. Even in the case that FPC is not in standby state due to maintenance, one RHR division is able to remove decay heat in both of the reactor and SFP. This would be the normal response to the fault but it is not the response claimed in the fault analysis. Therefore there is no corresponding HBSC.

If the loss of cooling is caused by SBO, CCF of AC power supply systems or CCF of essential service and support systems, these operator's actions above may not be possible.

(3) Analysis of Event

The analysis of this fault is presented in two parts:

- Thermal-hydraulic analysis
- Dose evaluation

(I) Thermal-hydraulic analysis

(a) Analysis Assumptions

Based on the above study on availability of safety systems, loss of operating RHR with loss of the same division of ECCS in operating state C-3 is analysed with the following conservative assumptions. The analysis conditions are shown in Table 24.10-6.

- Among the three RHR divisions, the operating RHR stops due to the initiating event and the other two RHRs are not available due to one in maintenance and a single failure of the other. (Loss of all RHRs)
- Among the two FPC divisions, the operating FPC stops due to the initiating event and the other FPC division is not available due to either maintenance or a single failure. (Loss of all FPCs)
- Among the two HPCF divisions, one train is not available due to the initiating event and the remaining one is not available due to maintenance or a single failure.
- Among three LPFL divisions, all LPFLs are not available due to low S/P water inventory. (Loss of all ECCS)
- Among the two FLSS divisions, one division of the FLSS can be used for water injection to the reactor and SFP but the other FLSS is not available due to maintenance.
- FLSR and Fire Protection System are available if necessary but are not considered in the analysis.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

- AC-W1: RPV water level shall be maintained above the TAF of the reactor core during shutdown to prevent the fuel being uncovered and heating up.
- AC-W2: SFP water level shall be maintained above the TAF of the spent fuel pool to prevent spent fuel being uncovered and heating up.
- AC-D3: Dose to workers should be less than 200 mSv.

AC-D4: Dose to members of the public should be less than 10 mSv.

(c) Fault Progression

Following loss of the operating RHR with loss of the same division of the ECCS during reactor shutdown modes, the fault progresses as follows:

- (i) Loss of operating RHR and FPC.
- (ii) The water temperature increases.
- (iii) The water level decreases due to boil-off of coolant in the reactor well.
- (iv) The standby RHR, HPCF, LPFL, and FPC all fail to start due to maintenance or a single failure.
- (v) Water injection from the FLSS is manually initiated after 30 minutes from receipt of the alarm by the operators in order to recover the water level.
- (vi) The water level recovers and the controlled state is achieved.
- (vii) After 7 days, the decay heat removal function is assumed to be restored and safe shutdown state is achieved.

It is assumed that the operators manually initiates FLSS to make up the water being lost when the reactor well water level reaches the SFP low water level alarm (18.2 hours) and before the level drops to TAF (several days). Apart from the alarm on low water level, RHR operating state is indicated in the MCR and the abnormal state is immediately noticed by the operator. In addition, there will also be radiation alarms plus the fact that hundreds of m³ of steam are being generated. The probability that the operators would fail to diagnose that initiation of FLSS was necessary is very low.

It is noted that, in case that failure of FLSS is assumed in this event, FLSR or Fire Protection System can be credited as effective injection systems. As shown in the result of this event, event progress is relatively slow and thus there is enough time margin for the operators to take countermeasures for the fault. Therefore, although it will take relatively longer time to prepare FLSR or Fire Protection Systems ready for use (such as line-up and manual valve operation), the time margin is sufficient to allow the operators to take the appropriate actions required. This scenario is provided only in the low frequency event, such as CCF of Class 1 systems.

(d) Analysis Results

Table 24.10-7 shows the event sequences. The temperature of reactor well water reaches 100 °C in 15.7 hours and the water level starts to decrease due to boil-off until the SFP low water level alarm is triggered. The change of the water level is shown in Figure 24.10.2-7. At 18.7 hours when the water injection by one train of the FLSS starts, the water level has decreased by 0.2 m. The FLSS water

injection recovers the full water level of the reactor well and its level is maintained thereafter. The FLSS maximum water injection rate to the RPV (1100 m³/h) is capable of recovering the decreased water volume, calculated as approximately 86 m³, and the water level thereby recovers over a short time. The RHR and FPC are recovered after seven days from the event occurrence, and a safe shutdown state is achieved.

Operator action as described above means that the water level in the reactor and SFP remains no lower than the SFP low water level alarm setpoint, which is significantly above the TAF in both locations so that AC-W1 and AC-W2 are met.

Table 24.10-7: Event Sequence of Loss of Operating RHR with Loss of the Same Division of ECCS (Operating state C-3)

Time	Event
0 hour	Loss of operating RHR and FPC occurs.
15.7 hours	Water temperature in the reactor well reaches 100 °C, and the water level starts decreasing.
>15.7 hours	Steam generation leads to pressure rise in Reactor Building. Depending on leakage and heat losses, the R/B blowout panel may open to vent the steam to the environment.
18.2 hours	Reactor well water level reaches the SFP low water level and the alarm is triggered in the MCR.
18.7 hours	Water injection with FLSS is started after 30 minutes from SFP low water level alarm by the operators
18.8 hours	The water level is recovered.
7 days (168 hours)	RHR and FPC are restored and safe shutdown state is achieved.

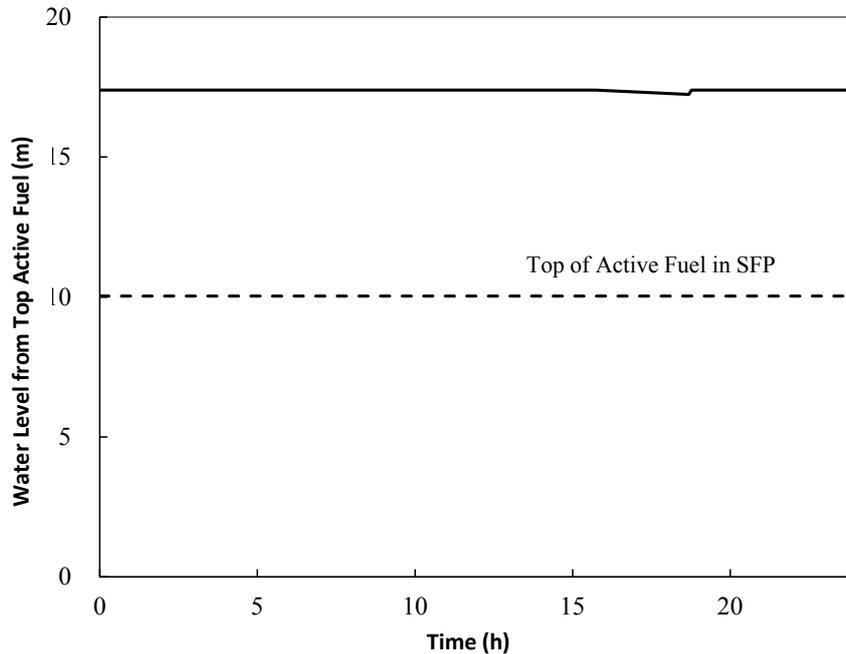


Figure 24.10.2-7: Water Level in Loss of Operating RHR with Loss of the Same Division of ECCS (Operating state C-3)

(II) Dose Evaluation

The evaluation of the radiological consequences for the loss of operating RHR with loss of the same division of ECCS includes dose evaluation for operators on the on-site locations, as well as for the public off-site. Dose evaluation for workers on the operating deck is not considered because there is more than 10 hours from occurrence of the initiating event by the time of coolant boiling starts, and the workers can evacuate from the operating area to outside of the operating deck without receiving additional dose.

(a) Analysis Assumptions

Figure 24.10.2-8 shows the release and transport pathway for radionuclides assumed for the dose analysis for the event. The radionuclides either from the evaporating water of the reactor and SFP are released to the Reactor Building (R/B) operating deck, and subsequently to the environment at ground level. The relevant design basis source term from Chapter 20 and 23 for the activity levels in the reactor and SFP water are used in the analysis. It is assumed that steam generation and radioactive carry-over occur at the same rate for seven days until cooling is restored.

(b) Analysis Results

It is assumed that steam generation occurs for 7 days and that a significant proportion of the deposit on the fuel (DB Deposition Source Term (DST)) is released due to boiling and carry-over. A smaller part of the dose is assumed to come from tritium in the water. The pathways for public exposure are shown in Figure 24.10.2-8. The release to the environment is mainly from leakage from the R/B. Even though the blowout panel is located near the R/B roof, all the release is assumed to be at ground level irrespective of the exact pathway. It is conservatively assumed that no deposition of radioactive material is assumed as the steam is released (DF=1).

The calculated doses using these conservative assumptions are shown in Table 24.10-8.

The worker dose is less than BSO and significantly less than the 200 mSv required by AC-D3. The public dose is greater than the BSO but less than the 10 mSv required by AC-D4. Because the public dose > BSO, it is in the tolerable-if-ALARP region. As a result a detailed ALARP study has been completed [Ref-35] to ensure that the risk is ALARP.

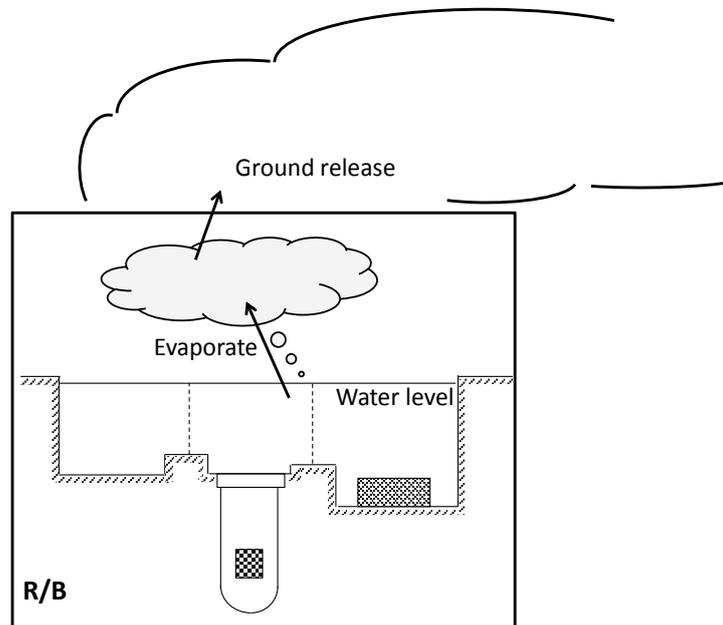


Figure 24.10.2-8: Release Pathway for Radionuclides during Loss of Decay Heat Removal Event in Reactor Shutdown Modes

Table 24.10-8: Doses to Exposed Persons from Loss of Decay Heat Removal Event in Shutdown Modes (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	5.9E-01	5.1E-01	6.0E-01	AC-D4 (BSL): 1.0E+01 BSO: 1.0E-02
On-site (Control Room)	-	-	6.6E-02	AC-D3 (BSL): BSL: 2.0E+02 BSO: 1.0E-01

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that the acceptance criteria described above are met for this event as follows:

- The lowest water level in the reactor and SFP is 0.2 m lower than the SFP normal water level, and it is higher than the TAF for the reactor core, spent fuel and the fuel handled by the FHM. Therefore, fuel integrity is maintained. These results satisfy AC-W1 and AC-W2 with significant margin.
- The on-site dose for workers in the control room is 0.07 mSv which is lower than AC-D3.
- The off-site dose is conservatively evaluated as 0.6 mSv which is lower than AC-D4.

Although AC-D4 is met for public dose, the dose is > BSO and, therefore, only acceptable if it is shown to be ALARP. A detailed ALARP assessment was carried out for this fault [Ref-35]. Firstly, the calculated off-site dose is very conservative:

- A very high fraction of radioactive material deposited on the fuel is assumed to be resuspended during boiling and carried over in the steam
- No deposition of material in the R/B is credited
- The release is assumed to be at ground level when, in fact, it would be at least at operating deck level

Taking these effects into consideration would lead to a best estimate dose close to BSO.

Secondly, a number of options that might reduce this off-site were identified and evaluated. None of the options considered had the potential to reduce an already low best-estimate dose, that is, none were deemed to be reasonably practicable. Therefore the risk from this event is assessed as being ALARP.

24.10.2.2 Loss of Reactor Coolant in reactor shutdown modes

All events which are categorised as loss of reactor coolant in reactor shutdown modes are summarised in the following list:

- Draindown due to valve failure within operating RHR (Fault Schedule Ref: 13.7)
- LOCA at feedwater line inside PCV (Fault Schedule Ref: 13.8)
- LOCA at RHR suction line inside PCV (Fault Schedule Ref: 13.9)
- LOCA at LPFL return line inside PCV (Fault Schedule Ref: 13.10)
- LOCA (mechanical) below TAF (Fault Schedule Ref: 13.11)
- RPV draindown by CUW (Fault Schedule Ref: 13.12)
- Leakage during FMCRD inspection (Fault Schedule Ref: 13.13)
- Leakage during replacement ICM nozzle (Fault Schedule Ref: 13.14)
- Leakage during RIP inspection (Fault Schedule Ref: 13.15)
- Refuelling Bellows Perforation caused by an Irradiated Fuel Drop (Fault Schedule Ref: 13.16)
- LOCA at CUW system line outside PCV (Fault Schedule Ref: 13.17)
- LOCA at RHR system line outside PCV (Fault Schedule Ref: 13.18)
- Inadvertent opening of all ADS due to spurious failure of Class 1 SSLC (Fault Schedule Ref: 11.4.2)

A representative event in the loss of reactor coolant fault group in reactor shutdown modes is “LOCA at RHR suction line inside PCV” in “Operating state C-3”. This is designated as an infrequent fault.

In addition, “Leakage during ICM nozzle replacement” is additional representative event because re-close operation of the PCV hatches and airlocks in the lower drywell is necessary for this fault scenario. This is designed as an frequent fault.

The detailed evaluations for all cases above are shown in Attachment-J of the “Topic Report on Design Basis Analysis” [Ref-5].

24.10.2.2.1 LOCA at RHR suction line inside PCV

Fault Schedule Ref: 13.9

(1) Description of Fault

This fault causes loss of the operating RHR and reactor draindown from the normal water level or the full reactor well level to the elevation of RHR suction line nozzle. The water level could possibly decrease toward the elevation of the RHR suction line. Since hatches in the lower drywell are assumed to be open during the operating state C-3, outflow water from the RHR suction line could flow into the R/B through the lower drywell, and therefore flooding in the R/B could occur. In addition, generated steam in the reactor and the SFP could be released to the operating deck. Continuous steam release to the operating deck could affect one division of RHR.

In the RHR suction line LOCA fault inside the PCV, the reactor and SFP water level decreases and pre-operated RHR shutdown cooling is assumed to be lost due to the initiator. After the reactor and SFP cooling are lost, boiling of the reactor well water cannot be prevented. The reactor well and SFP boiling could eventually lead to uncovering of the reactor core and spent fuel in the SFP leading to fuel damage and a large release of activity. However, even in the case of LOCA, there are diverse and independent means of introducing water to the reactor and SFP:

- HPCF (Class 1) – Automatic initiation is available, and operator initiation is also claimed in the fault assessment and is covered by HBSC HF HPCF 2-3.1 and HBSC HF SSLC 2-3.1 (see Table A-2 of this chapter, and details for Chapter 27, Appendix A)
- LPFL (Class 1) – Automatic initiation is available, and operator initiation is also claimed in the fault assessment and is covered by HBSC HF SSLC 2-3.1.2 (see Table A-2 of this chapter, and details for Chapter 27, Appendix A)
- FLSS (Class 2) - Operator initiation is claimed in the fault assessment and is covered by HBSC HF FLSS 2-3.1 and HBSC HF FLSS 2-3.2 (see Table A-2 of this chapter, and details for Chapter 27, Appendix A)
- FLSR or Fire Protection System (Class 3) – In the event that FLSS is unavailable (considered in BDB event), operator initiation of FLSR or Fire Protection System provides the necessary makeup. This is covered by HBSC HF FLSR 2-3.1 (see Table A-2 of this chapter, and details for Chapter 27, Appendix A).

An operator initiates the standby HPCF, LPFL or FLSS to maintain the water level. The operator controls the injection flowrate to the reactor to prevent the consequential effect of R/B flooding to the remaining safety divisions.

(2) Plant Normal Response

In a loss of reactor coolant event in shutdown modes, the operator initiates the standby HPCF or LPFL to maintain water level and initiate RHR to remove decay heat. Here, either one of the three independent RHR divisions is lined up in S/P cooling mode or LPFL mode. In addition, when the SFP gate is open, the operator initiates the standby FLSS to maintain water level in the SFP. Although the SFP can be made-up by FLSS but not be sufficiently cooled, steam could be generated in the SFP and be released to the operating deck. Consequentially, one division of Class 1 safety systems could be lost due to effect of the steam. However, at least one division of Class 1 safety systems is not affected and can be available for cooling the reactor core and SFP.

Re-close operation of personnel airlocks and hatches will be conducted by workers to prevent consequential effects to the safety SSCs in the R/B, if it is practicable.

(3) Analysis of Event

The analysis of this fault is presented in two parts:

- Thermal-hydraulic analysis
- Dose evaluation

(I) Thermal-hydraulic analysis**(a) Analysis Assumptions**

Referring to the study on availability of safety systems, LOCA at RHR suction line inside PCV in operating state C-3 is analysed based on the following conservative assumptions:

- (i) A piping break of RHR suction line inside the PCV is assumed to occur.
- (ii) The operating RHR (in shutdown cooling mode) division is lost due to the initiating event.
- (iii) Among the three RHR divisions, one RHR is lost due to steam release in the operating deck, and the other two RHRs are not available due to maintenance or a single failure. (Loss of all RHR)
- (iv) Among the two HPCF divisions, all HPCFs are lost due to maintenance or a single failure.
- (v) Among the two LPFL divisions, one LPFL is lost due to consequential effect of steam release in the operating deck, and the other two LPFLs are not available due to maintenance or a single failure. (Loss of all ECCS)
- (vi) Among the two FLSS divisions, one FLSS can be used for water injection to the reactor and the SFP. Another FLSS is assumed to be in-maintenance.

(b) Acceptance Criteria

The acceptance criteria are given in section 24.3.3. For this event, they are:

- AC-W1: RPV water level shall be maintained above the TAF of the reactor core during shutdown to prevent the fuel being uncovered and heating up.
- AC-W2: SFP water level shall be maintained above the TAF of the spent fuel pool to prevent spent fuel being uncovered and heating up.
- AC-D5: Dose to workers should be less than 500 mSv.
- AC-D6: Dose to members of the public should be less than 100 mSv.

(c) Fault Progression

Following the postulated break of an RHR suction line inside the PCV in operating state C-3, the fault progresses as follows:

- (i) Reactor coolant is lost by the break in the RHR suction line inside the PCV.
- (ii) The water level decreases.
- (iii) The alarm at SFP low water level is triggered.
- (iv) Water injection from the FLSS to the reactor and SFP is manually initiated after 30 minutes from the SFP low water level alarm.
- (v) The water level reaches the height of the SFP weir and the SFP is isolated from the reactor.
- (vi) The reactor water level reaches to the elevation of the break line nozzle.
- (vii) The reactor and the SFP water level is maintained above the TAF.

(d) Analysis Results

Table 24.10-9 shows the event sequence, and Figure 24.10.2-9 shows the time variation of the water level.

At one minute after the event initiation, the water level reaches the SFP low water level, and the operator in the MCR recognises an anomaly by the triggered alarm. The water level continues to decrease and at 30 minutes after the SFP low water level alarm, the FLSS injection into the reactor and SFP is manually initiated. However, the water level continues decreasing and at 52 minutes after event initiation, the water level reaches the SFP weir, and the RPV is then isolated from the SFP, resulting in maintenance of cooling of the fuel in the SFP by the FLSS injection water. Since the SFP is sufficiently cooled from this point, the analysis concentrates on the behaviour of the RPV hereafter.

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

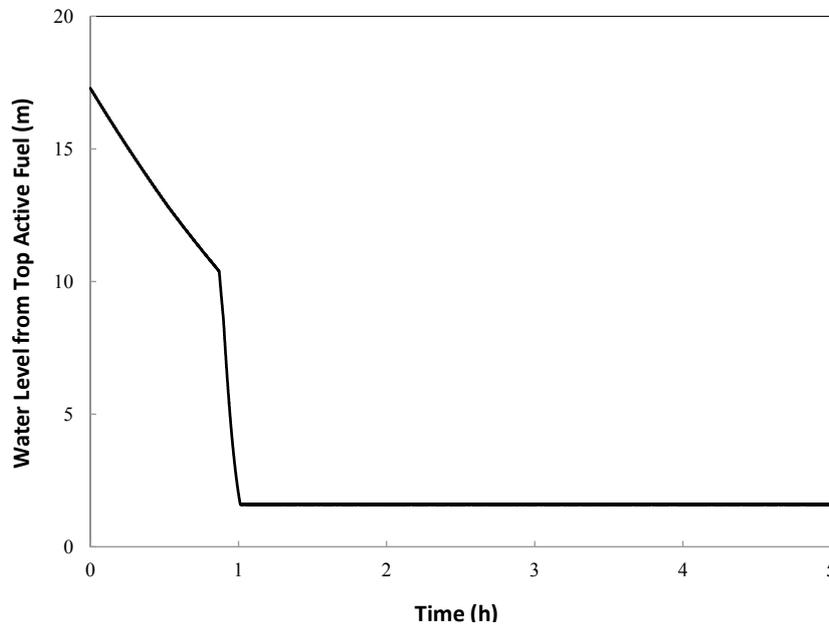
When the reactor is isolated, the water level continues to decrease toward the elevation of the nozzle connected to the break line. Finally, at 61 minutes after the event initiation, the water level reaches the nozzle elevation. Thereafter, the reactor water level is maintained at the nozzle elevation, and the SFP water level is maintained at the elevation of SFP weir. The operator controls the injection flow rate to make up the decreased reactor water evaporated by the decay heats to maintain the reactor and SFP water level above TAF.

In addition to the above, in the operating state C-3, operation of fuel handling by the FHM is considered. One step of the overall fuel transportation process is assumed to take three minutes after the occurrence of the initiating, and further steps are not started. As a result, at the completion time of transportation (i.e., three minutes after occurrence of the event), the water level in the SFP is 25.9 m from bottom of RPV and higher than TAF of the handled fuel. Therefore, exposure of the fuel assembly from the reactor/SFP water surface does not occur during the fuel transportation.

NOT PROTECTIVELY MARKED

**Table 24.10-9: Sequence of Events for LOCA at RHR Suction Line inside PCV
(Operating state C-3)**

Time	Event
0 minute	Loss of reactor coolant occurs.
1 minutes	Alarm is triggered at the SFP low water level.
32 minutes	FLSS injection is manually initiated at 30 minutes after the SFP low water level alarm.
52 minutes	The SFP is isolated from the reactor and the SFP water level is maintained by the FLSS injection.
61 minutes	The reactor water level decreases to nozzle elevation of the break line (10.7 m from bottom of RPV)) and the reactor water level is maintained by the FLSS injection.



**Figure 24.10.2-9: Water Level in Case of LOCA at RHR Suction Line inside PCV
(Operating state C-3)**

(II) Dose Evaluation

Evaluation of the radiological consequences of the LOCA at RHR suction line inside PCV includes dose evaluation for operators on the operating deck. The fault is assumed to cause draindown of the reactor well. However, the result of the water level calculation shows that fuel damage does not occur in this fault. In addition, this fault causes water evaporation in the reactor and SFP because the reactor and SFP water level decreases to the elevation where the RHR shutdown cooling mode and FPC cooling cannot be restarted during the event. The dose evaluation for steam generation is similar to that for loss of decay heat removal shown in Section 24.10.2.1. The dose of workers on the other on-site location, as well as for the public off-site could slightly larger than the case, but there is enough margin against dose criteria. Thus, these dose are not considered in this fault.

(a) Analysis Assumption

In terms of decrease in water level in the reactor, DSP (dryer/separator pit) and SFP, it is assumed that the level decreases at the same rate since the reactor well gate is open. Table 24.10-10 shows assumed locations of equipment, taking account of conservatism. It is noted that calculation results are compiled as ‘Reactor and DSP’ and ‘SFP’ in this section. The effective direct doses are calculated using time change of water level shown in Figure 24.10- 9. The operators on the working floor of the Fuel Handling Machine (FHM) are assumed to be above the central axis of the radiation source. The workers operating on the FHM would immediately recognise the decrease in water level in the reactor well due to the LOCA. It is assumed that the initiating event occurs during transportation of a fuel assembly. The transportation motion of the FHM still continues and finishes the current step of fuel transportation. Thus, the workers start evacuation after completion of the current transportation step. The time taken for the worker evacuation from the operating area to outside of the operating deck based on the above assumptions is evaluated as six minutes. This assumption includes the time for pre-movement action by workers for decision/preparation for evacuation.

Table 24.10-10: Locations of Components

Location	Components
DSP	Separator (Shroud Head and Separator) and Dryer
RPV	Reactor Fuel, Top Guide
SFP	Spent Control Rod Storage, Spent Fuel Storage and Spent Fuel Assembly Transport

(b) Analysis Results

Dose evaluation is carried out for a worker on the FHM with the source being the SFP internal (Spent fuel). The calculated doses using these conservative assumptions are shown in Table 24.10-11. The worker dose is less than BSO and AC-D5.

Table 24.10-11: Doses to Exposed Persons from LOCA inside PCV in Shutdown Modes (mSv)

Location	Adult	Dose Criteria
On-site (Operating deck)	3.3E-02	AC-D5 (BSL): BSL: 5.0E+02 BSO: 1.0E-01

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the acceptance criteria are met for this event as follows.

- The lowest water level in the RPV is 10.7 m from the bottom of the RPV and higher than the TAF. The lowest water level in the SFP is the SFP weir height which is higher than the TAF of the spent fuel. The lowest water level in the RPV and the SFP during fuel transportation is 25.9 m from the bottom of RPV and higher than the TAF of handled fuel. Therefore, fuel integrity is maintained. These results satisfy AC-W1 and AC-W2.
- Workers start evacuation immediately after the LOCA event and evacuation is completed in approximately six minutes. On this basis, the worker dose is below the AC-D5 criterion value. This result satisfies AC-D5.
- The off-site dose is estimated as 0.6 mSv from the result of loss of decay heat removal event, and is lower than AC-D6.

Although AC-D5 and AC-D6 are met for public dose, these dose are > BSO and, therefore, only acceptable if it is shown to be ALARP. It is demonstrated that all the design basis acceptance criteria are met with significant margins.

Firstly, although AC-D5 is met for worker dose, the dose is > BSO. In this case, the pipe assumed to break is designed as Class 1 component and the fault frequency is extremely low. In addition, in shutdown modes, the reactor pressure boundary is not pressurised and therefore a line break is unlikely to occur. Therefore, in fact, the fault frequency is equivalent to BDB events but evaluated as an infrequent design basis fault for conservative purposes. With regard to analysis conditions, a

guillotine break is conservatively assumed, and thus the speed of the draindown is evaluated with conservative margin.

Secondly, although AC-D6 is also met for public dose, the dose is $>$ BSO and the risk from steam generation is shown to be ALARP in Section 24.10.2.1. Moreover, in the analysis, loss of RHR is assumed at the event initiation. However, in fact, RHR can be used for core cooling for a certain time until RHR is affected by steam generated from the SFP. Therefore, the evaluated amount of steam released to the environment is conservative.

In addition, there is enough time margin to take action and there are also Class 2 and Class 3 systems available to use for making up reactor coolant in this event. The defence in depth provided by these lower class systems and the margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

24.10.2.2.2 Leakage during Replacement ICM Nozzle

Fault Schedule Ref: 13.14

(1) Description of Fault

Leakage due to the cumulative effect of a number of incorrect operations during ICM nozzle replacement is assumed. This fault causes RPV draindown in the same way as 24.10.2.1. Since the considered leakage occur at a lower level than the Top of Active Fuel in the RPV, this fault could lead to the RPV draindown from the initial water level to below the core. The event is an example of LOCA below TAF. In this event, the reactor water is discharged directly to the lower drywell. The discharging flow rates is estimated to be smaller than that in other LOCA events represented in 24.10.2.2.1, there is enough time margin to start makeup of the reactor well using water injection systems, and once injection system is initiated, water level can be increased and maintained at the full of reactor well. However, if the recovery operation to terminate leakage is assumed to fail, the leakage continues and then the lower drywell could be flooded. Subsequently, since the lower drywell is in the open state during an outage, the water inflows into the R/B via the access tunnels.

Continuous inflow of water into the R/B will lead to consequential effect of internal flooding of safety divisions, and eventually all RHR for long-term heat removal could be lost. Therefore, the open hatch and airlock in the lower drywell are required to be closed in order to prevent the consequential effects on the long term heat removal safety function and to terminate loss of water inventory to outside the PCV.

(2) Plant Normal Response

In a loss of reactor coolant event caused by human error, the workers terminate leakage in accordance with correct recovering operation. The operating RHR division continues operation and therefore a cooled state for the reactor and SFP is ensured. However, when the recovering operation fails, discharge of water into the lower dry well is not terminated, and thus hatch and personnel airlock in the lower drywell must be closed by the workers. In LOCAs below TAF, assumed leakage flow is small, and decrease speed of water level is very slow. Thus, there is enough time margin to start water injection until the water level decreases to below the TAF in the reactor or SFP, comparing to the LOCA case treated in Section 24.10.2.2.1.

(3) Analysis of Event**(a) Analysis Assumptions**

Referring to the study on availability of safety systems, the leakage caused by human error in operating state C-3 is analysed based on the following conservative assumptions:

- (i) A leakage at the RPV bottom in pedestal side due to cumulative incorrect operation of workers is assumed to occur.

- (ii) Operating RHR continues operation.
- (iii) Recovering operation of the leakage by the operator fails, and discharge of water into the lower drywell continues.
- (iv) Water level is maintained at the full of reactor well by operator's action.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, they are:

- AC-W1: RPV water level shall be maintained above the TAF of the reactor core during shutdown to prevent the fuel being uncovered and heating up.
- AC-W2: SFP water level shall be maintained above the TAF of the spent fuel pool to prevent spent fuel being uncovered and heating up.
- AC-D1: Dose to workers should be less than 20 mSv.
- AC-D2: Dose to members of the public should be less than 1 mSv.

(c) Fault Progression

Following the postulated leakage caused by human error in reactor shutdown modes, the fault progresses as follows:

- (i) A leakage occurs at the RPV bottom in pedestal side due to the cumulative effect of a number of incorrect operations by workers.
- (ii) The water level in the reactor well decreases, while in the lower drywell increases.
- (iii) Closing of the lower drywell is started by the workers.
- (iv) The alarm on SFP low water level is triggered.
- (v) Water injection to the reactor and SFP is manually initiated, and the water level is maintained.
- (vi) Closing of the lower drywell is completed.

(d) Analysis Results

In the case that an In-core monitor is assumed to be uninstalled by the operator in the fuel handling area and the In-core monitor nozzle coordinates is withdrawn at the pedestal, the reactor draindown occurs and the coolant inflows to the lower drywell. The workers operating on the operating deck and in the lower drywell would immediately recognise the initiating event. The reactor well water level is assumed to be made up and maintained at the full of reactor well by operator action. In this case, it takes about four hours from occurrence of the initiating event for the flooding into the R/B via the access tunnels to occur. The time margin is sufficient to allow the workers to complete closure of the lower drywell before the flooding occurs.

Since the minimum water level is sufficiently high, the direct radiation effect is negligible small. Thus, the additional dose for the workers in the operating deck does not occur. In addition, the reactor cooling state continues during the event, and thus the radiological consequences due to steam generation do not occur. Furthermore, worker dose during closing of the lower drywell has to be considered but is negligibly small.

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that the acceptance criteria described above are met for this event as follows:

- The progress of this event is much slower than that for Section 24.10.2.1 because the assumed discharged flow is much smaller than that for Section 24.10.2.1. Therefore, the water level is maintained above TAF by operator's action and fuel integrity is maintained. This result satisfies AC-W1 and AC-W2.
- Worker dose on the operating deck is negligible small, and the results satisfy AC-D1 and the BSO.
- Worker dose during closing operation of the lower drywell is negligibly small. This result satisfies AC-D1. In addition, this fault does not cause water evaporation and therefore there is no impact on off-site dose. These results satisfy AC-D1 and AC-D2, and the BSO.

It is demonstrated that all the design basis acceptance criteria are met with significant margins. Although this analysis is carried out based on the conservative assumption, the result shows that closing of the lower dry well before the flooding in the R/B occurs is reasonably practicable. The margins before acceptance criteria might be threatened contribute to the claim that the risks from this event are ALARP.

24.11 Analysis Results and Fault-based View – Non-Reactor Faults

Outside the reactor, the principal inventories of radioactive material are associated with the SFP and fuel route (handling, storage and export of spent fuel) and the handling and storage of radioactive waste. This section considers faults in these two areas:

- SFP and Fuel Route faults – see Section 24.11.1
- Radioactive Waste System leaks or failures – see Section 24.11.2

24.11.1 SFP and Fuel Route Faults

This section presents results of transient analysis and dose evaluation for representative design basis faults associated with the SFP and Fuel Route to demonstrate adequacy of the safety design and suitability and sufficiency of the safety measures. The detailed evaluations for all cases are reported in the Topic Report on Design Basis Analysis for the SFP and Fuel Route [Ref-15].

Three representative faults are considered:

- Loss of SFP cooling (loss of all FPC Pumps) – see Section 24.11.1.1 (Fault Schedule Ref: 14.1)
- Fuel handling accidents (drop of spent fuel assembly during refuelling) – see Section 24.11.1.2 (Fault Schedule Ref: 14.5)
- Cask handling accidents (spent fuel cask drop during spent fuel export) – see Section 24.11.1.3 (Fault Schedule Ref: SFIS.3.1)

All of these are considered as infrequent Design Basis faults

(1) SFP Faults

The SSCs providing HLSFs required for SFP faults are shown in Table 24.11-1.

The analysis conditions for SFP faults in shutdown modes are shown in Table 24.10-6.

Table 24.11-1: SSCs providing HLSFs for SFP Faults

HLSF	SSC	PCSR Ref	Notes
1-9 Functions to maintain sub-criticality of spent fuel outside the reactor coolant system	SFP racks (Class 1)	19.8.2.1	SFP racks maintain sub-criticality of storage fuel in all operating modes.

Table 24.11-1: SSCs providing HLSFs for SFP Faults (Continued)

HLSF	SSC	PCSR Ref	Notes
2-4 Functions to cool spent fuel outside the reactor coolant system	SFP (Class 1)	19.8	The SFP maintains the coolant for fuel cooling.
	FPC (Class 1)	19.9	FPC is a two division Class 1 system proving cooling to SFP during all normal operating modes, Heat is rejected to RCW and RSW
	RHR (Class 1)	12.3.5.4	RHR is a three division Class 1 system proving cooling to the reactor during shutdown modes. Heat is rejected to RCW and RSW. Power for RHR is provided by EDG. RHR provides the FPC with supplemental fuel cooling in the event of a full core offload. This function can also be used for recovery from potential upper pools cooling failure and subsequent boiling event.
	SSLC (Class 1)	14.6.2.1	SSLC provides the functions to control SSCs related to FPC and RHR.
2-5 Functions to make up water for spent fuel pool	FLSS (Class 2)	16.7.3.1	FLSS provides makeup water into the SFP in the event of loss of decay heat removal.
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to FLSS.
4-7 Functions to confine radioactive materials, shield radiation, and reduce radioactive release	Check valve and Syphon breaker system (Class 1)	19.9.1.2	The check valves and syphon break system prevents potential syphon from the SFP and subsequent spent fuel exposure in the SFP.
5-2 Supporting functions especially important to safety	Class 1 EPS (Class 1)	15.3	Class 1 EPS supplies power to Class 1 SSCs. EDG supports SSCs related to RHR and FPC.
	RCW/RSW (Class 1)	16.3.2	RCW/RSW are essential systems for supporting FPC, RHR and Class 1 HVAC operations.
	UHS (Class 1)	16.3.1	UHS provides sufficient cooling water to the RSW.

Table 24.11-1: SSCs providing HLSFs for SFP Faults (Continued)

HLSF	SSC	PCSR Ref	Notes
5-3 Function of alternative supporting system	B/B Class 2 EPS (Class 2)	15.4.6	Class 2 EPS supplies power to the second line of safety systems. BBGs supports SSCs related to FLSS.
	EECW (Class 2)	16.3.6	EECW supplies recirculation cooling water to BBG auxiliaries.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 1 HVAC (Class 1)	16.5	Class 1 HVAC ensures the adequate environmental parameters for Class 1 SSCs are maintained.
	HECW (Class 1)	16.3.5.1	HECW provides chilled water for Class 1 HVAC.
	Class 2 (A2) HVAC (Class 2)	16.5	Class 2 (A2) HVAC ensures the adequate environmental parameters for SSCs related to SLC are maintained.
	HBCW (Class 2)	16.3.5.3	HBCW provides chilled water for Class 2 (A2) HVAC.

Table 24.11-2: Analysis Conditions for SFP Faults

Items	Analysis conditions
Fuel type	10 × 10 Fuel (GE 14)
Fuel operation cycle condition	17 month operation and 30 days outage
Elapsed time from reactor shutdown	16 days
Decay heat	3.35MW (Normal heat load (NHL) condition) 9.75MW (Maximum heat load (MHL) condition)
Initial water level	SFP normal water level
Initial water temperature	52°C (NHL condition) 65°C (MHL condition)
FLSS flow (rated value for SFP injection)	120 m ³ /h
Initiation signal of water injection for SFP	SFP low water level alarm
SFP activity level	SFP DB Source Term as defined in Chapter 20

Limits and Conditions for Operation

The future licensee shall ensure that, in all operating modes, the following plant condition is maintained:

- The SFP water level shall be above the low water alarm level

The future licensee shall ensure that, during normal power operation, no more than one division of the following systems and their support systems in the same division shall be subject to testing or maintenance:

- FPC
- SSLC
- Class 1 EPS
- EDG
- RCW
- RSW
- UHS
- Class 1 HVAC
- HECW
- FLSS
- HWBS
- B/B Class 2 EPS
- BBG
- EECW
- Class 2 (A2) HVAC
- HBCW

The future licensee shall ensure that, in all operating modes, the following SSC is operational:

- Check valve and Syphon breaker system

The future licensee shall ensure that, in all operational modes, the SFP activity is below the DB SFP Source Term as defined in Chapter 20.

(2) Fuel Route Faults except for Faults during Spent Fuel Export

SSCs providing HLSFs required for SFP faults are shown in Table 24.11-3.

Table 24.11-3: SSCs providing HLSFs for Fuel Route Faults

HLSF	SSC	PCSR Ref	Notes
5-6 Functions to handle fuel and heavy equipment safely	FHM (Class 1)	19.6	FHM has duel load path and Class 1 protection to prevent fuel drop accidents.
	FHM (Class 1 and Class 2)	19.6	FHM, associated lifting attachments and safety systems handle irradiated loads suitably submerged so that radiation shielding is provided. The length of each lifting attachment is appropriate so that when the RIP Inspection Hoist upper limit is reached, the workers are not subject to unacceptable doses
	RBC (Class 1)	19.7	RBC has duel load path and Class 1 protection to prevent fuel drop accidents
	RBC (Class 2)	19.7	RBC, associated lifting attachments and safety systems handle irradiated loads suitably submerged so that radiation shielding is provided.
4-7 Function to confine radioactive materials	Secondary Containment (Class 2)	13.3.4.1	Radioactive materials are collected within Secondary Containment and treated before release to the environment by SGTS if fuel drop or drop of heavy equipment fault occurs. .
	R/A HVAC isolation damper (Class 2)	16.5	R/A HVAC isolation damper is closed to form Secondary Containment.
	SGTS (Class 2)	13.3.4.2	SGTS controls the emission of radioactive materials by maintaining a negative pressure in the Secondary Containment and by filtering the effluent prior to discharge to the atmosphere if fuel drop or drop of heavy equipment fault occurs.
	Temporary Shielding Equipment * (Class 3)	19.3.2	The temporary shielding equipment reduces the worker dose in the upper drywell in case of drop of irradiated fuel.

* The use of Temporary Shielding Equipment will be considered at the site specific stage.

Table 24.11-3: SSCs providing HLSFs for Fuel Route Faults (Continued)

HLSF	SSC	PCSR Ref	Notes
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	SACS (Class 2)	14.6.4	SACS provides the functions to generate actuation signals for SSCs related to SGTS.

Limits and Conditions for Operation

The future licensee shall ensure that, during normal refuelling operation, the following SSC is operational:

- FHM Class 1 and Class2 protection system
- RBC Class 1 and Class2 protection system
- Secondary Containment
- R/A HVAC isolation damper
- SGTS
- SACS

24.11.1.1 Loss of SFP cooling (Loss of All FPC Pumps)

Fault Schedule Ref: 14.1

(1) Description of Fault

In any operating mode, in the extreme circumstance where the operating FPC pump trips and the standby FPC pump fails to start, the fuel cooling ability of the SFP is lost and the SFP water temperature increases and could potentially lead to SFP water boiling and a decrease in SFP water level. If this loss of water is not made up, this would ultimately lead to uncover of the fuel and fuel damage. This extreme event is considered as a severe accident in Chapter 26.

During normal operation, heat is removed from the SFP by FPC, which keeps the SFP water temperature below 100°C.

In the case of loss of FPC, the large amount of water in the SFP provides sufficient time margin with regards to SFP accident management before the boiling of SFP water and the uncover of spent fuel. More specifically it takes 27 hours (Normal heat load condition) and 7 hours (Maximum heat load condition) for the SFP water to start to boil. In addition, it takes approximately 330 hours (Normal heat load condition) and approximately 110 hours (Maximum heat load condition) for the SFP water level to reach TAF of SFP storage rack if there is no water injection. This time margin allows manual operation for backup or recovery action.

Even if the SFP water starts boiling, the spent fuel damage can be avoided by water makeup. In this case, the FLSS, which has an independent power source and a dedicated line for the injection of water into the SFP, can be used for SFP makeup. The FLSS has two redundant pump divisions and it can be operated manually from the Main Control Room (MCR) and the Backup Building (B/B) with corresponding HBSC HF FLSS 2-5.1 (see Chapter 27 Appendix A).

Moreover the Flooding System of the Reactor Building (FLSR), which also has a dedicated injection line, can also be used for makeup in case of FLSS failure.

(2) Plant Normal Response

In a loss of SFP cooling event, the operator initiates the standby FLSS or lower class water injection systems such as FLSR or the Fire Protection System, MUWC and SPCU to maintain water level until the FPC can be recovered.

(3) Analysis of Event

The analysis of this fault is presented in two parts:

- Thermal-hydraulic analysis

- Dose evaluation

(I) Thermal-hydraulic analysis

(a) Analysis Assumptions

The following assumptions are used in the analysis:

- (i) The decay heat is conservatively assumed to be constant during the transient, although in practice it decreases with time.
- (ii) Two cases of initial SFP conditions, Normal Heat Load (with quarter core and 200% of core spent fuel) and Maximum Heat Load (with a full core and 200% of core spent fuel), are assumed.
- (iii) Although the full core offload condition is not a regular operation, it has been evaluated to explore a more severe scenario. In this case, it is assumed that the RHR is used to remove the massive amount of decay heat generated.
- (iv) It is assumed that that operator would recognise the FPC failure by the operation condition display or announcements in the MCR and by the failure of all recovery actions performed during the large time margin available. The operator would also recognise the SFP water level decreasing and initiate the FLSS injection by the SFP water level switch and related announcement indicating SFP water loss. Conservatively, in this case, only the SFP water level switch is credited.
- (v) The FLSS can inject sufficient water to make up the loss of water due to the water boiling caused by decay heat.
- (vi) Water injection by the FLSS starts after 30 minutes from the alarm in order to recover the water level.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

AC-N1: k_{eff} shall be smaller than 0.95 to maintain sub-criticality in the SFP.

AC-W2: SFP water level shall be maintained above the TAF of the spent fuel pool to prevent spent fuel being uncovered and heating up.

AC-D3: Dose to workers should be less than 200 mSv.

AC-D4: Dose to members of the public should be less than 10 mSv.

(c) Fault Progression and Analysis Results**(i) Normal Heat Load condition**

- 1) The SFP water temperature starts increasing and the water reaches the boiling point approximately 27 hours after the cooling failure. After that, the SFP water level decreases due to boil-off and reaches the “SFP water level low” set point at approximately 33 hours after the event, and then the water level alarm is initiated. The operator would recognise the alarm and starts to prepare for FLSS injection. FLSS can make up sufficient water and the SFP water level will be recovered.
- 2) The spent fuel criticality remains within the condition of “Criticality Analysis for the Fuel Storage Rack” so sub-criticality is maintained, whose result is evaluated in Attachment A of [Ref-15].

(ii) Maximum Heat Load condition

The SFP water temperature starts increasing and the water reaches the boiling point approximately 7 hours after the cooling failure. After that, the SFP water level decreases due to boil-off and reaches the “SFP water level low” set point at approximately 9 hours after the event, and then the water level alarm is initiated. The operator would recognise the alarm and starts to prepare for FLSS injection. FLSS can make up sufficient water and the SFP water level will be recovered. The water level variation is shown in Figure 24.11.1-1.

The spent fuel criticality remains within the conditions of “Criticality Analysis for the Fuel Storage Rack” so sub-criticality is maintained, whose result is evaluated in Attachment A of [Ref-15].

(II) Dose Evaluation**(a) Public Dose**

In this event, the steam including a tiny amount of radioactive materials is assumed to be released from the SFP to the environment through the blow-out panels, although, for conservatism, the release is assumed to be at ground level. The mass of steam release from the SFP over a period of 7 days is evaluated as approximately 700 tonnes in the normal heat load conditions and as approximately 2230 tonnes in the maximum heat load conditions, respectively. In this case, the impact of radiation dose to the public due to a loss of SFP and/or Reactor well cooling is evaluated in Attachment D of [Ref-15]. As reported in Attachment D, the result of public dose is 6.0E-1 mSv in the conditions that the mass of steam release is assumed to be 2880 tonnes, (which is a bounding value taking account of a SFP gate open condition and bounding steam generation). It can be seen from this analysis that radiation dose to the public is much lower than the AC-D4 (10 mSv).

(b) Worker Dose

The radiation level for the workers on the operating deck increases when the SFP water level decreases. However, there are at least 27 hours (Normal heat load condition) and 7 hours (Maximum heat load condition) time margins before the SFP water starts to boil off, and therefore the workers would evacuate from the operating deck before the decrease of SFP water level by acting on the alarm of high SFP water temperature. Hence, the worker on the operating deck does not receive an additional radiation dose associated during this event.

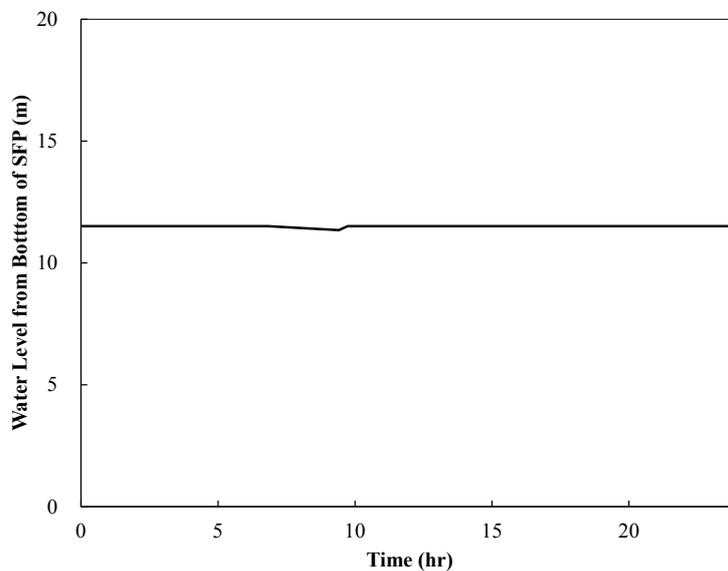


Figure 24.11.1-1: Water Level in Loss of Decay Heat Removal Event (Maximum Heat Load Condition)

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria described above, it is demonstrated that all the acceptance criteria are met for this event as follows.

- The lowest SFP water level is 11.1 m for the maximum heat load condition and that is greater than the top of active fuel (TAF) in the SFP. This result satisfies acceptance criterion AC-W2.
- The spent fuel criticality remains within the conditions of “Criticality Analysis for the Fuel Storage Rack” and therefore sub-criticality is maintained during the event. This result satisfies acceptance criterion AC-N1.
- After the occurrence of the loss of cooling function event, workers start evacuation before the

water level starts to lower. Thus, the workers do not receive an additional dose for this event. This result satisfies acceptance criterion AC-D3.

- The off-site dose is evaluated as $6.0E-1$ mSv in operating state C-3 which is the most onerous condition, which is lower than the AC-D4 acceptance criterion value.

A specific ALARP study was performed for this event [Ref-35] and the risks were shown to be ALARP.

24.11.1.2 Fuel Handling Accident (FHA – drop of spent fuel assembly during refuelling)

Fault Schedule Ref: 14.5

(1) Description of Fault

The FHM is designed to enable a fuel assembly to be transferred under water, with enough depth to effectively shield the radiation from the irradiated fuel in the SFP. The FHM is designed to prevent a fuel assembly dropping during transferring operations. However, this event could be caused if multiple failures occur such as a double wire failure. This fault is assumed to be an infrequent fault.

A fuel handling accident (FHA) on the spent fuel storage pool is bounded by a FHA over the core since fuel still in the core has less decay time. Therefore, an explicit analysis for the spent fuel pool case has not been performed.

The UK ABWR has the following countermeasures to protect against this fault:

- (i) The FHM is designed to prevent fuel drop.
- (ii) The FHM's vertical over movement is limited by an interlock.
- (iii) The FHM's horizontal movement is limited by a position detector.
- (iv) The FHM has derailment prevention lugs so that it will not fall down in a design earthquake.
- (v) Even if a drop of fuel occurs, the operator would immediately recognize the fact and would evacuate from the operating deck.
- (vi) If a drop impact causes mechanical fuel damage and a subsequent release of fission products from damaged fuel rods, the reactor building HVAC exhaust isolation damper is automatically closed on a "High Radioactivity in operating deck area monitor" signal in the radiation monitoring system.

(2) Protection against the Fault

The normal response of the plant is automatic isolation of the Reactor Building and automatic initiation of the SGTS on detection of high radioactivity in fuel handling area to maintain the secondary containment and to treat and reduce the radioactive substance to be discharged to the environment.

(3) Analysis of Event

(a) Analysis Assumptions

The following assumptions are used in the analysis:

- (i) The accident occurs at a time after shutdown identified in the technical specifications as the earliest time fuel handling operations may begin. Radioactive decay of the fission product inventory during the interval between shutdown and commencement of fuel handling operations are taken into consideration.
- (ii) The drop of a fuel assembly occurs when fuel assemblies are being manipulated over the reactor core for refuelling, and the fuel assembly falls on top of the core impacting a group of four assemblies.
- (iii) The drop impact causes mechanical fuel damage and a subsequent release of fission products from damaged fuel rods.
- (iv) Gases pass from the water to the operating deck.
- (v) The R/A HVAC isolation damper is automatically closed a “High radioactivity in operating deck area monitor” via the radiation monitoring system.
- (vi) The SGTS operation is also automatically initiated by the same signal.
- (vii) The operator evacuates from the operating deck after recognition of the area radiation monitor alarm and/or electronic personal dosimeter.
- (viii) The release and transport pathway for this event is shown in Figure 24.11.1-2. The radionuclides are dispersed in the operation deck area from the failed fuel through the reactor water. Since the R/B ventilation system isolates immediately, the contamination is processed by the SGTS and subsequently released to the environment from the plant stack. Radioactivity decay in the reactor building corresponding to the SGTS flow rate is considered, and the decontamination factor provided by the reactor water is considered.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, they are:

AC-N1: k_{eff} shall be smaller than 0.95 to maintain sub-criticality in the SFP.

AC-D3: Dose to workers should be less than 200 mSv.

AC-D4: Dose to members of the public should be less than 10 mSv.

(c) Fault Progression

The fault progression of the FHA is as follows:

- (i) During a refuelling operation, a fuel assembly is moved over the top of the reactor core. While the fuel assembly is over the core, a failure occurs allowing the assembly, the fuel grapple mast, and head to fall on top of the core impacting a group of four fuel assemblies.
- (ii) Some fuel rods in both the dropped and struck assemblies fail, releasing radioactive gases

into the reactor water.

- (iii) Gases pass from the reactor water to the R/B fuel-handling area.
- (iv) The R/B Operational Floor high radiation alarm alerts plant personnel and automatically initiates isolation of the R/B Heating, Ventilation, and Air Conditioning system and the start of the SGTS.

(d) Analysis Results

(i) Evaluation of amount of damaged fuel

The amount of fuel damaged because of a drop of an irradiated fuel assembly is evaluated and it is conservatively assumed that a maximum of two bundles are damaged or 184 GE14 fuel rods.

(ii) Evacuation time

The evacuation time of the operator on the operating deck is evaluated using the evacuation time model. In the evacuation time model, event initiation, alarm initiation and pre-movement activities are considered. As a result, the evacuation time is evaluated as approximately four minutes.

(iii) Dose evaluation

Table 24.11-4 shows dose evaluation results for the fuel drop accident, indicating that off-site dose is almost the same as the BSO and on-site dose (in the control room) is lower than the BSO. In addition, during fuel handling, entrance to the operating deck by workers other than the FHM operator is prohibited. Therefore, the worker dose on the operational deck is expected to be less than the AC-D3 criterion value.

(iv) Sub-criticality in case of fuel drop

The k_{eff} for a single bundle is less than 0.50. Sub-criticality is maintained when fuel is dropped into the core or the spent fuel pool, because the distance between the fuel in the reactor or SFP and dropped fuel is more than the neutron mean free path.

Table 24.11-4: Doses to Exposed Persons from Fuel Drop Accident (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	1.7E-02	1.6E-02	1.6E-02	AC-D4 (BSL): 1.0E+01 BSO: 1.0E-02
On-site (Control Room)	-	-	1.2E-02	AC-D3 (BSL): 2.0E+02 BSO: 1.0E-01
On-site (Operational deck)	-	-	1.9 E+01	

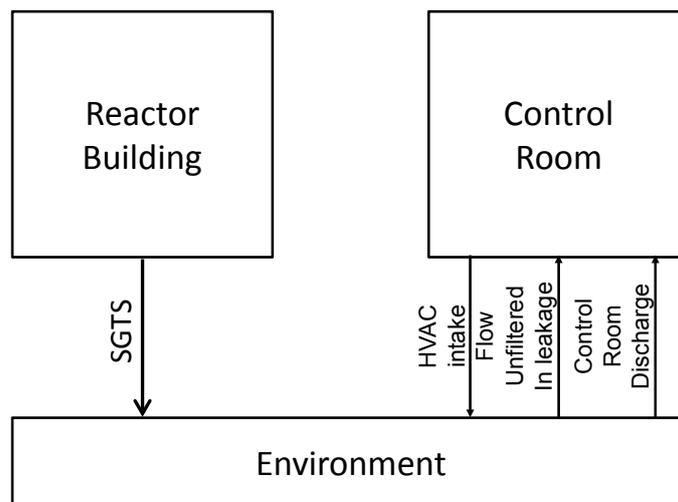


Figure 24.11.1-2: Fuel Handling Accident Release to Environment

(4) Discussion and Conclusions

From the comparison between the analysis results and the acceptance criteria, it is demonstrated that all the acceptance criteria are met for this event.

The modelling of this event has some large conservatisms such as the assumption on the number of damaged fuel pins. In addition, the FHM has Class 1 protection to prevent events that might lead to the drop of a fuel assembly other than gross failure of the FHM or of the fuel assembly itself, both of which are very unlikely. It is therefore deemed that there are no further reasonably practicable measures that can be adopted to reduce risk and that the risk is therefore ALARP.

24.11.1.3 Cask Drop Accident

Fault Schedule Ref: SFIS.3.1

Fuel is exported from the SFP to interim storage (SFIS) using a transfer cask. Fuel is loaded into the canister in the cask pit and, once filled, the transfer cask containing loaded canister is raised onto the cask stand so that the lid can be welded on. After this, the cask is moved via the hoist well to the truck bay, where this potential cask drop fault might occur. It is then loaded to a transporter for removal from the R/B. All of these processes are managed using the Reactor Building Overhead Crane (RBC). The SSCs providing the required HLSFs for these processes are shown in Table 24.11-5.

Table 24.11-5: SSCs providing HLSFs for Spent Fuel Export

HLSF	SSC	PCSR Ref	Notes
1-10 Functions to maintain sub-criticality of spent fuel during processes of spent fuel removal from cask pit to storage area and during interim storage period	Canister Basket (Class 1)	19.10	The canister basket will be designed to provide passive protection against criticality.
2-6 Functions to maintain spent fuel temperature limit during processes of spent fuel removal from cask pit to storage area and during interim storage period	Canister(Class 1) CCS (Class 1) BCCS (Class 2) OPTS (Class 1)	19.10	The canister will be designed to provide the necessary heat transfer from the spent fuel.
4-14 Functions to provide containment barrier during processes of spent fuel removal from cask pit to storage area and during interim storage period	Canister (Class 1)	19.10	The canister will be designed to provide the necessary containment for spent fuel in conjunction with impact limiter.
4-16 Functions to provide radiation shield during processes of spent fuel removal from cask pit to storage area and during interim storage period	Canister (Class 1) Transfer Cask (Class 1)	19.10	The canister will be designed to provide the necessary shielding.
5-6 Functions to handle fuel and heavy equipment safely	FHM (Class 1) RBC (Class 1) Lifting Attachment (Class 1)	19.6 19.7 19.7	FHM and RBC handle loads safety.

Table 24.11-5: SSCs providing HLSFs for Spent Fuel Export

HLSF	SSC	PCSR Ref	Notes
5-16 Functions to provide handling and retrievability during processes of spent fuel removal from cask pit to storage area and during interim storage period	Canister (Class 1) Transfer Cask Load Path (Class 1) Cask stand (Class 2)	19.10	RBC has dual load paths and Class 1 protection to prevent drops.
5-22 Function to limit deceleration loading to canister containment boundary during credible cask drop faults	Impact limiters (Class 1)	19.10	Impact limiter is installed in truck bay to protect the canister containment barrier.

Limits and Conditions for Operation

The future licensee shall ensure that, prior to cask campaign, the following SSCs are operational:

- RBC Class 1 protection system
- Impact limiter

(1) Description of Fault

In this fault, the RBC is assumed to fail during one of the lifting operations:

- Lowering the cask from the operating floor to the truck bay via the hoist well

This results in the cask falling and impacting the truck bay floor. Both the cask pit and truck bay floor have impact limiters to protect the cask in the case of a drop. Depending on the type of failure, the fall may be a free fall of the cask or an uncontrolled descent whilst still attached to the crane.

In principle, failure of the RBC can be from mechanical failure of the crane bridge, failure of the load path or failure of the crane control system or by some impact, snagging or ledging event causing the load to become detached from the crane. In [Ref-39] [Ref-40], these faults are shown to be infrequent faults.

The crane control and protection systems are designed to prevent impact, snagging and ledging. The protection system is a Class 1 system with two redundant divisions. Mechanically, the crane is designed to nuclear crane standards and has redundant load paths. As the crane is a Class 1 SSC, dropping of a transfer cask is an infrequent fault. Dropping the cask in the host well to the truck bay (21m potential fall) is the bounding case.

(2) Plant Normal Response

If the fault occurred because of failure of the control system, the crane protection system would prevent the uncontrolled fall of the cask.

(3) Analysis of Event (Dose Evaluation)**(a) Analysis Assumptions**

It is assumed that the cask and canister are the same as those described for use in the SFIS in Chapter 32, correctly loaded with 89 spent fuel elements cooled in the SFP for 10 years.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, the relevant acceptance criteria are:

- AC-D3 Dose to workers should be less than 200 mSv for initiating event frequencies between 1×10^{-3} and 1×10^{-4} /y.
- AC-D4 Dose to members of the public should be less than 10 mSv for initiating event frequencies between 1×10^{-3} and 1×10^{-4} /y.
- AC-C2 Canister deceleration following a DB drop shall remain below allowable limit.

(c) Fault Progression

The fault is initiated by a failure of the RBC which allows the cask to fall in an uncontrolled manner either freely or whilst still connected to the crane. The drop height to the operating deck is limited by the crane control and zoning system. Drops in the cask pit or hoist well are protected by impact limiters.

(d) Analysis Results

The behaviour of the cask has been assessed [Ref -41] with the cask falling in all orientations onto the impact limiter in the truck bay with the fall being the entire height of the hoist well. In all cases, the deceleration experienced by the cask on impact with the impact limiter was less than the allowable deceleration limit (60g for the conceptual design). Acceptance criterion AC-C2 is therefore met.

Because the deceleration is less than the allowable limit, the cask is deemed not to fail so there is no release of activity from fuel in the cask, even though the fuel itself may be damaged in the fall. The fact that the cask is not damaged also means that it maintains its shielding function thereby protecting the operator's present from direct dose above normal operational dose targets. Therefore,

both criteria AC-D3 and AC-D4 are met.

Further, the fact that Acceptance Criterion AC-C2 is met ensures that the canister is able to provide the other HLSFs to maintain the temperature and sub-criticality of the fuel.

(4) Discussion and Conclusions

For this infrequent fault all the relevant Acceptance Criteria are met. The bounding case (drop of a spent fuel transfer cask in the hoist well) has been subject to a detailed ALARP assessment [Ref -42] [Ref-43] and the arrangement described in this chapter based on a Class 1 RBC and impact limiter has been found to be the ALARP case, that is, no other options were deemed to be reasonably practicable.

24.11.2 Radioactive Waste System Leak or Failure

The Radioactive Waste System handles radioactive waste in solid, liquid and gaseous forms. In terms of off-site doses and indirect worker doses, the gaseous and liquid radioactive waste systems are dominant.

Two representative faults are considered in this section:

- Discharge of gaseous waste (Off-Gas system failure) – see Section 24.11.2.1
- Discharge of liquid waste (Liquid radioactive waste leak or failure) – see Section 24.11.2.2

SSCs providing HLSFs required for radioactive waste faults are shown in Table 24.11-6.

Table 24.11-6: SSCs providing HLSFs for Radioactive Waste Handling and Storage

HLSF	SSC	PCSR Ref	Notes
4-7 Functions to confine radioactive materials, shield radiation, and reduce radioactive release	TVTS (Class TBC *)	18.9	Tank Vent Treatment System (TVTS) uses HEPA filters
	Normal HVAC (Class 3)	16.5	
4-8 Functions to minimise the release of radioactive gas	OG isolation valve (Class 2)	18.7	OG is isolated from Condenser on receipt of high radiation or high temperature area alarm
4-11 Functions to store the radioactive materials as gaseous waste	OG (Class 3)	18.7	OG confines noble gases and iodine in charcoal filters
4-12 Functions to store the radioactive materials as liquid wastes	LWMS (Class TBC *)	18.5	

* LWMS and TVTS are only concept designs in GDA

Limits and Conditions for Operation

The future licensee shall ensure that, during normal operations, the following SSCs are operational:

- OG isolation valve
- T/B HVAC
- Rw/B HVAC
- TVTS

24.11.2.1 Off-Gas Treatment System Failure

Fault Schedule Ref: 15.1

The Off-Gas (OG) system draws non-condensable gases from the main condenser, principally to maintain the condenser vacuum. These gases consist of:

- air from leakage into the condenser
- hydrogen and oxygen from radiolysis and injected as part of the water chemistry regime
- nitrogen-16 from activation of oxygen in the reactor core
- noble gases and iodine from pin-hole fuel failure

The OG system has recombiners to remove the hydrogen and oxygen from the off-gas and charcoal beds to hold up noble gases and iodine to allow decay before release to the environment via the stack.

The OG system has Class 2 automatic isolation valves in the event of failure of the system integrity, which isolates the system from the condenser and stops steam being supplied to the Steam Jet Air Ejectors (SJAEs) giving diverse means of stopping gas flow through the system - see Table 24.11-6.

(1) Description of Fault

In this fault, the OG system pipework is assumed to fail leading to release of the off-gas stream to the rooms in the Turbine Building (T/B) containing the system components. Two events are considered as representative events: pipe rupture at the outlet of the first stage SJAe and Charcoal Adsorber break. In each case, noble gases and iodine are assumed to be released to the environment at ground level leading to doses to workers and the public. The fault analysis is described in Attachment L of [Ref-5].

The Charcoal Adsorbers are operated with negative pressure, so the release of radioactive substances may not occur with a small rupture. However, it is conservatively assumed that a complete failure of the Charcoal Adsorber occurs and all the contained radioactive substances within the Charcoal Adsorber are released.

Given the low pressures in the OG system and based on structural integrity assessment of the system, these faults are designated as infrequent faults with frequency between $1E-4$ /y and $1E-5$ /y.

As far as the reactor is concerned, this fault is the same as closure of MSIVs (Fault Schedule ID 2.1). In this section, the concern is public and worker exposure to radiation from the failure of the OG system.

(2) Plant Normal Response

The normal response of the plant is automatic isolation of the OG system on detection of high radiation levels or high temperature in the OG rooms as in the fault described here. The operator closes the MSIVs manually leading to a trip of the turbine and reactor. Gas and steam released from the failed component would normally be removed from the room by the T/B HVAC to the stack.

(3) Analysis of Event

(a) Analysis Assumptions

- (i) As there is no fuel failure expected during normal operation, the FP fission product concentration in the Off-Gas source term is assumed to be the conservative value derived from the MSLB assessment and given in the common source term for radiological consequence analysis in Chapter 20.
- (ii) The released radioactivity instantaneously mixes into the Turbine Building atmosphere from where it is released to the environment without holdup as a ground level release.
- (iii) The break is located in the pipe before the charcoal beds in the Off-gas system such that there is no hold up of the radioactivity in the system.
- (iv) It is assumed that OG isolation valve is closed in 16 minutes automatically because of an OG area radiation level high signal.
- (v) The operator closes the MSIV manually in 30 minutes following the OG area radiation level high alarm to isolate the FP release from the system.
- (vi) For the retention effect in the building, a decontamination factor of 10 is assumed for nuclides other than noble gas and organic iodine.
- (vii) No credit is taken for decay time in the T/B or HVAC or release from the stack.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is an infrequent fault, they are:

AC-D5: Dose to workers should be less than 500 mSv.

AC-D6: Dose to members of the public should be less than 100 mSv.

(c) Fault Progression

The release of radioactive gas and steam from the pipe rupture or Charcoal Absorber failure fills the room in which the failure occurs.

The gas is assumed to build up in the room where the break occurs until OG isolation valve (Class 2) is automatically actuated after 16 minutes of the break on receipt of one or both of:

- OG component area radiation high alarm
- OG component area temperature high alarm

The 16 minutes response time of OG isolation is because of the time needed to detect the radiation rise from a small leak.

(d) Analysis Results

The concentration of nuclides in the Off-gas source term is conservatively assumed to the same as for the MSLB event (see Section 24.8.4.1) and described in Chapter 20 and 23. Noble gas in the main steam is extracted by the SJAE from the main condenser, so all of the noble gas is considered in the source term. A significant amount of the main steam inventory is retained in the condensate water in the main condenser and only a negligibly small fraction is carried over.

The gas is assumed to be released through building structures to the environment as shown in Figure 24.11.2-1 and not through the HVAC system to the stack.

Three scenarios are considered:

- Exposure of members of the public from gases released to the environment at ground level
- Exposure of workers in adjacent rooms from gases moving between rooms
- Exposure of operators in the MCR from gases entrained into the MCR HVAC

The results are given in [Ref-5] Attachment L and in Table 24.11-7.

Table 24.11-7 Dose results for OG system faults

Item	Members of the public off-site			MCR operator	Operator in adjacent room
	1y	10y	Adult		
OG System Rupture (mSv)					
Total	2.9E-01	9.9E-02	5.1E-02	3.9E-03	Bounded by absorber break
Charcoal adsorber break (mSv)					
Total	7.0E+00	2.1E+00	7.9E-01	4.6E-02	2.0E+00

The largest dose to a member of the public is 2.9E-01 mSv which is above BSO for the NSEDP Target 4 but is significantly below the BSL and meets the acceptance criterion AC-D6 with a large margin. Similarly, the largest worker dose is 2.0E+00 mSv, which again is above the BSO for Target 4 but significantly below the BSL and meets acceptance criterion AC-D5 by a very large margin.

(4) Discussion and Conclusions

The doses to workers and the public from this event meet the acceptance criteria with a large margin. However, because the doses are above BSO, they are only acceptable if they can be shown to be ALARP. A specific ALARP assessment has been performed for the OG system and the doses have been shown to be ALARP as there are no reasonably practicable means of reducing them [Ref-36].

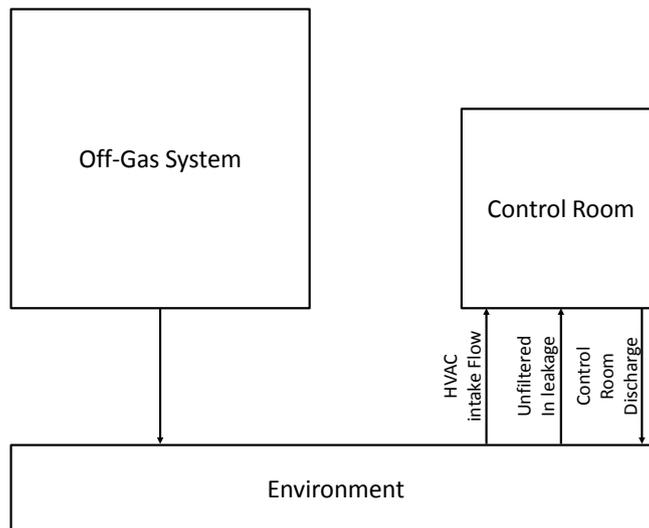


Figure 24.11.2-1: Off-Gas System Failure Release to Environment

24.11.2.2 Liquid Radioactive Waste System Faults

24.11.2.2.1 Liquid Radioactive Waste System Leak or Failure

Fault Schedule Ref: 15.2

(1) Description of Fault

The analysis of the radiological consequences for the Liquid Radioactive Waste System Leaks or Failure assumes a failure of the Powder Resin Storage Tank in the Liquid Radioactive Waste System that discharges the entire inventory of the tank to the tank cell, although no credit is taken for the cell in the analysis. Postulated events that could cause a release of the inventory of a tank are sudden unmonitored cracks in the pipework, valve failure or operator error. Small cracks and consequent low-level releases are bounded by this analysis.

This event bounds releases from

- LCW collection tank
- HCW collection tank
- LD collection tank
- Filter sludge storage tank
- Bead resin storage tank
- Concentrated waste system tank

all of which are covered by Fault Schedule reference 15.2. The liquid radioactive waste tanks are assumed to be designed to Class 3. Therefore, the fault is treated as a frequent fault.

There are no claimed SSCs in the analysis of this event. However, Table 24.11-8 shows Class 3 defence in depth measures to reduce off-site dose and no LCOs are identified.

Table 24.11-8: Provision of HLSFs for Powder Resin Storage Tank leakage

HLSF	System	PCSR reference	Notes
4-7 Functions to confine radioactive materials, shield radiation, and reduce radioactive release	Ejector	–	Class 3 defence in depth measure to all transfer of leaked liquid – only affects long term release
	Leak detector alarm	–	Class 3 defence in depth measure

(2) Plant Normal Response

There is no plant normal response assumed for this fault except normal operation of the Radioactive Waste Building HVAC.

(3) Analysis of Event

(a) Analysis Assumptions

- (i) The release and transport pathway for this accident is shown in Figure 24.11.2-2. A single pathway is considered for release of fission products to the environment via airborne releases. The liquid pathway is not considered due to the mitigative capabilities of the Radioactive Waste Building. For the airborne pathway, volatile iodine species are considered for long term release due to evaporation.
- (ii) The design basis process source term for the powder resin storage tank as defined in Chapter 20, sub-section 20.3 (Definition of Radioactive Sources) is assumed.

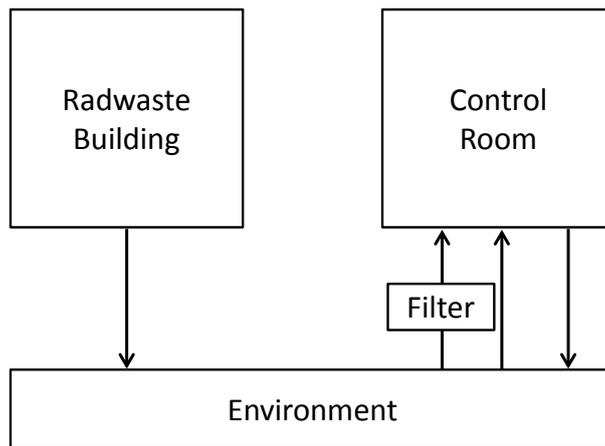


Figure 24.11.2-2: Radioactive Waste System Leak or Failure Release to Environment

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

AC-D1: Dose to workers should be less than 20 mSv.

AC-D2: Dose to members of the public should be less than 1 mSv.

(c) Fault Progression

This analysis assumes that an unspecified event causes the complete release of the radioactive inventory in the Powder Resin Storage Tank. Postulated events that could cause a release of the inventory of a tank are sudden unmonitored cracks in the vessel or operator error. In this case, there is also release to the environment. Ground level release of gaseous radioactive species is assumed which contaminates the air flowing into the Control Building.

(d) Analysis Results

There are three scenarios to be considered in the dose assessment for this fault:

- Exposure to the public by release to the environment with ground level release.
- Exposure to workers in the C/B Main Control Room through air intake to C/B as shown in Figure 24.11.2-2.
- Exposure to workers in the vicinity of the leak. This scenario is bounded by the SS Pipe Failure fault – see Section 24.11.2.2.2.

Table 24.11-9 shows dose evaluation results for the Liquid Radioactive Waste System leak or failure, indicating that off-site dose is below the BSL but above the BSO and on-site dose (in the main control room) is lower than the BSO.

Table 24.11-9: Doses to exposed persons from Radioactive Waste System Leak or Failure (mSv)

Location	1y age	10y age	Adult	Dose Criteria
Off-site	1.5E-01	4.0E-02	1.2E-02	AC-D6 (BSL): 1.0E+00 BSO: 1.0E-02
On-site (Control Room)	-	-	7.2E-04	AC-D5 (BSL): 2.0E+01 BSO: 1.0E-01

(4) Discussion and Conclusions

The risk to the C/B MCR operators is below BSO.

In the case of exposure of the public, the dose meets the Acceptance Criterion for the event. However, the dose is also above the BSO for the corresponding NSEDP risk target [Ref-24]. This means the risk is acceptable provided it is as low as reasonably practicable.

Firstly, it should be noted that the released inventory would be less than in the calculation because much of the resin, being solid, would remain in the tank. Secondly, release would not be at ground level in practice but would be via the HVAC, HVAC filters and stack. This would significantly reduce the dose exposure to the public compared to the assumption of ground-level release.

Furthermore, off-site dose and MCR worker dose can be reduced by the following accident management measures. If a release of liquid radioactive wastes occurs, the leak detector alarm notifies the operator in the main control room of a leak from the liquid radioactive waste tank. The operator starts to remove the spilled liquid to a standby tank by using the ejector from outside the tank cell.

In addition to this accident management measure, Chapter 18 identifies further measures that a future licensee may decide to adopt:

- Transfer into the tank can be stopped to minimise the leak
- Stack monitoring can provide additional means of detecting the leak as gaseous radioactive species are removed by the HVAC system to the stack

Neither of these options is foreclosed, and, given that the LRWS design is only conceptual in GDA, it is concluded that the risk from this fault is capable of being reduced to ALARP levels.

24.11.2.2.2 SS Pipe Rupture

Fault Schedule Ref: 15.3

(1) Description of Fault

The analysis of the radiological consequences for the SS pipe rupture assumes that the resin transfer piping from the Powder Resin Storage Tank to the Wet-solid ILW Processing System ruptures during the resin transfer process, and the leaked effluent spreads on the floor as shown in Figure 24.11.2-3. In this case, it is possible that a worker could enter the pump room next to the enclosed Powder Resin Storage Tank cell and receive additional direct radiation from the leaked liquid waste and internal exposure caused by its evaporation and by aerosol carry-over. It is noted that doses to the public and operators in the main control room (MCR) are not considered in this event because those doses are evaluated in Section 24.11.2.2.1.

This fault bounds releases during transfer from the CUW Backwash Tank to the Powder resin Storage Tank.

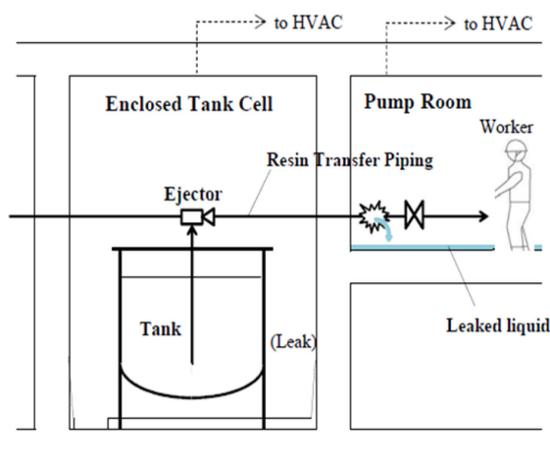


Figure 24.11.2-3: Outline of SS Pipe Rupture

The resin transfer piping (SS pipe) is designed to Class 3. The frequency of rupture is estimated to be between $1E-2$ /y and $1E-3$ /y as it is designed to operate at low pressure. It is assumed in the analysis that the transfer operation takes approximately 10 to 15 hours spread over the year. This means the time at risk is small. However, because of the failure rate of the piping and the potential consequences, for the purposes of analysis, the fault is treated as a frequent fault.

The main protection against this fault is the prevention of entry of workers into the pump room during transfer operations as shown in Table 24.11-10.

Table 24.11-10: Provision of HLSFs for SS Pipe Rupture Event

HLSF	System	PCSR reference	Notes
5-12 Functions to limit worker access into high dose area	Powder Resin Storage Tank pump room entry prevention	–	The exact form of entry prevention is part of ongoing access control design. (See assumption section in PCSR Chapter 18, Section 18.5.3.1)

Limits and Conditions for Operation

The future licensee shall ensure that, during normal operations, the following SSC is operational:

- Powder Resin Storage Tank pump room entry prevention

(2) Plant Normal Response

There is no plant normal response assumed for this fault except normal operation of the Radioactive Waste Building HVAC.

(3) Analysis of Event

(a) Analysis Assumptions

- (i) The design basis process source term for the powder resin storage tank as defined in Chapter 23 is assumed.
- (ii) It is assumed that transfer operations total 10 to 15 hours /y.
- (iii) For the airborne pathway, volatile iodine species are considered, for long term release due to evaporation. Chapter 18, Section 18.5.2.3 has also considered the short term release due to splashing and airborne entrainment. Note that the assessment presented here for fault 15.3 and that for the same fault in Chapter 18, Section 18.5.2.3 lead to the derivation of the same safety function category.

(b) Acceptance Criteria

The acceptance criteria are given in Section 24.3.3. For this event, which is a frequent fault, they are:

AC-D1: Dose to workers should be less than 20 mSv.

(c) Fault Progression

It is assumed that the resin transfer piping from the Powder Resin Storage Tank to the Wet-solid ILW Processing System ruptures during the resin transfer process and the leaked effluent spreads on the floor as shown in Figure 24.11.2-2. In the unmitigated case, it is assumed that an operator may enter the pump room adjacent to the powder resin storage tank cell when the spill occurs. Under these circumstances, the operator would receive a dose from direct radiation and internal exposure through inhalation.

(d) Analysis Results

The unmitigated dose uptake by an operator in the pump room is assessed as >500 mSv, whatever the event frequency.

The unmitigated dose to an operator entering the pump room is unacceptable and requires protective measures. As the time at risk is very short (10 to 15 hours per year), a single means of protection is reasonably practicable to prevent operator entry whilst transfer operations are in progress.

(4) Discussion and Conclusions

Transfer of resins from the Powder Resin Storage Tank to the Wet-solid ILW Processing System is a necessary operational procedure and the resulting short period of elevated risk is unavoidable. It is assumed that, for operational reasons, the period of elevated risk is as short as reasonably practicable.

The fault is only formally treated as a frequent fault. In reality, as the time at risk is very small – 120 to 130 hours per years - the effective frequency of the event is around $1.1E-5y$, which would put the fault just inside the design basis. However, it is recognised that from an ALARP point of view it is not acceptable to rely solely on the time-averaged risk being low. As a result, the implementation of a single Class 1 measure to prevent operator access to the pump room during resin transfer operations seems to be a reasonably practicable measure commensurate with the unmitigated risk being above BSL for a very short time.

Chapter 18 identifies a number of other potential means to reduce risk:

- Safe system of work to prevent operator entry to pump room
- The use of PPE/RPE
- Installation of activity-in-air alarm
- Installation of area gamma alarm

None of these options is foreclosed, and, given that the LRWS design is only conceptual in GDA, it is concluded that the risk from this fault is capable of being reduced to ALARP levels.

24.12 Performance of Class 2 SSCs in Frequent Faults

For frequent faults, the NSEDPs require that there should be diverse protection for each high level safety function at least at Class 2 in addition to the Class 1 provision required for infrequent faults.

It is necessary to demonstrate that the reactor can be brought to a safe shutdown state using these Class 2 SSCs alone and that they provide the necessary diversity to the Class 1 SSCs.

Table 24.12-1 shows the Class 2 SSCs providing HLSFs relating to cooling to bring the plant to a safe shutdown state. The failure of Class 1 reactivity control for frequent faults is discussed in Section 24.9.1 on ATWS.

Table 24.12-1: Class 2 SSCs providing HLSFs for Fuel Cooling and Long-term Heat Removal

HLSF	SSC	PCSR ref	Notes
2-2 Function of alternative fuel cooling	RDCF FLSS (Class 2)	16.7.3.3 16.7.3.1	RDCF depressurises reactor so that FLSS can function. Power for RDCF is provided by B/B Class2 DC power supply system. Power for FLSS is provided by BBG.
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to RDCF and FLSS.
	RDCF (Switching Valve for SRV) (Class 3)	16.7.3.3	Switching valve for SRV is capable of opening SRV (RDCF) manually without power source to keep the RPV pressure low when RDCF is unavailable after 24 hours.
3-2 Functions of alternative containment cooling and decay heat removal	AC FCVS (Class 2)	16.7.3.3 16.7.3.1 13.3.3.4	Heat rejected by feed and bleed with containment venting via AC or FCVS.
	HWBS (Class 2)	14.6.3	HWBS provides the functions to control SSCs related to AC and FCVS.
5-1 Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	HWBS (Class 2)	14.6.2.1	HWBS provides the functions to generate actuation signals for the engineered safety features (FLSS and RDCF).

Table 24.12-1: Class 2 SSCs providing HLSFs for Fuel Cooling and Long-term Heat Removal (Continued)

HLSF	SSC	PCSR ref	Notes
5-3 Function of alternative supporting system	B/B Class 2 EPS (Class 2)	15.3	B/B Class 2 EPS including B/B Class2 DC power supply system supplies power to the second line of safety systems. BBG supports SSCs related to alternative fuel cooling and alternative long term heat removal.
	EECW (Class 2)	16.3.6	EECW supplies recirculation cooling water to BBG auxiliaries.
5-18 Function to maintain internal building environment appropriate for SSCs	Class 2 (A2) HVAC	16.5	Class 2 (A2) HVAC ensures the adequate environmental parameters for SSCs related to SLC are maintained.
	HBCW	16.3.5.3	HBCW provides chilled water for Class 2 (A2) HVAC.

Limits and Conditions for Operation

The following LCO is identified in addition to those in Section 24.6, Section 24.7, Section 24.9.1 and Section 24.9.2:

The future licensee shall ensure that, during normal power operation, the following SSCs are operational:

- RDCF (Switching Valve for SRV)

24.12.1 Demonstrating Diverse Provision of Fundamental Safety Functions for Frequent Faults

For design basis faults, the principal means of delivering Category A safety functions are provided by Class 1 SSCs. In addition, for frequent faults, the diverse means of delivering Category A safety functions are provided by Class 2 SSCs. It needs to be demonstrated for frequent faults that the diverse means (Class 2) are effective if the Class 1 systems are not available. Therefore, analyses in which the Class 1 systems are unavailable and the Class 2 systems are used instead are performed for plant transient analysis.

In this section, the effectiveness of the diverse Class 2 protective means considers provision for each Fundamental Safety Function. Hence the:

- Reactivity Control function
- Fuel Cooling function
- Long-term Heat Removal function

are demonstrated.

24.12.1.1 Demonstration for Reactivity Control Function

In these analyses, the Class 1 RPS scram is unavailable, and loss of the Class 1 RPS is an example of an Anticipated Transient without Scram (ATWS) event. ATWS analyses are presented in Section 24.9.1.

24.12.1.2 Demonstration of the Fuel Cooling Function

Fault Schedule Ref: 3.1.1

(1) Class 1 and Class 2 Systems

Table 24.12-2 shows the Category A Class 1 and Class 2 systems for the Fuel Cooling function for frequent faults. The Emergency Core Cooling System consists of RCIC, HPCF, and LPFL/ADS. Therefore, unavailability of the ECCS is assumed in the analysis and RDCF and FLSS are used to provide the function.

Table 24.12-2: A1 and A2 Systems for Fuel Cooling Function of the Frequent Faults

Category & Class	Safety Systems
A1	<ul style="list-style-type: none"> • RCIC • HPCF • SRV - Safety valve function
A2	<ul style="list-style-type: none"> • RDCF (Alternative SRV) • FLSS

(2) Evaluated Faults

The faults to be evaluated are chosen from the list of frequent faults in terms of decrease of reactor water level and increase of reactor power. Since “Loss of all feedwater flow” (Fault Schedule Ref: 3.1) bounds “Feedwater controller failure – Maximum demand” (Fault Schedule Ref: 1.4) in terms of comparison of the analysis results with the acceptance criteria, then “Loss of all feedwater flow” is the bounding fault.

(3) Acceptance Criteria

The infrequent fault acceptance criteria relating to fuel are used rather than the frequent fault criteria, as the combination of a frequent fault and unavailability of Class 1 fuel cooling function is deemed to be infrequent. The acceptance criteria are given in Section 24.3.3. For this event, which is considered as an infrequent fault, they are:

AC-F5: The calculated maximum fuel cladding temperature shall not exceed 1,200°C.

AC-F4: The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.

(4) Analysis Assumptions

The main analysis conditions are shown in Table 24.12-3.

Table 24.12-3: Main Analysis Conditions for Demonstration for Fuel Cooling Function

Items	Conditions	Remarks
Reactor thermal power	4005 MW	102% of rated power
Fuel rod peak linear heat generation rate	44.0 kW/m x 1.02	102% of operating limit
Core flow rate	47.0×10 ³ t/h	90% of rated flow
Dome pressure	7.17 MPa [gauge]	Based on 102% of rated power
Decay heat	ANS/ ANSI-5.1-1971 + 20%	
Reactor initial water level	Normal water level	
Off-site power	Available	
Opening pressure of Safety Relief Valve (SRV)	Setpoint × 1.03	
FLSS		
Flow rate (1 train)	0 m ³ /h 660 m ³ /h 1100 m ³ /h	At 1.6 MPa [dif] * At 1.0 MPa [dif] * At 0.0 MPa [dif] *
Actuation signal	Low reactor water level (Level 1)	
Delay timer	10 min	
RDCF		
Actuation signal	Low reactor water level (Level 1)	
Delay timer	10 min	

*: MPa [dif] : differential pressure between the reactor pressure vessel and water source

(5) Analysis Results

The sequence of events for the fault is shown in Table 24.12-4. Analysis results are shown in Figure 24.12.1-1.

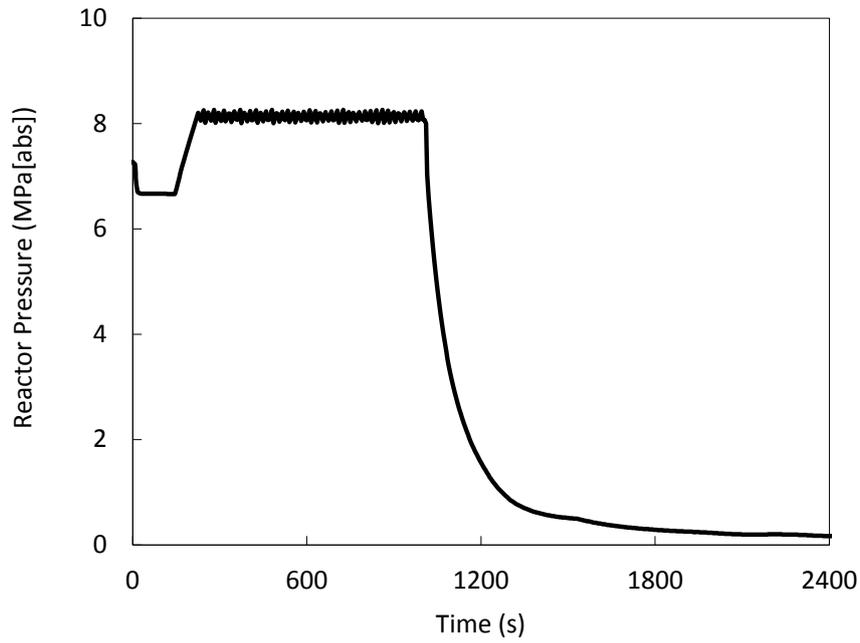
Due to the loss of all feedwater flow, the reactor water level decreases. When the reactor water level reaches low Level 1, after a 10 minute delay, the RDCF is actuated, and when the vessel pressure decreases below the FLSS shutoff head, FLSS begins water injection. The reactor core becomes partially uncovered but becomes covered again when the water level increases on FLSS initiation.

The PCT is about 527 °C and so is lower than the 1200 °C limit. The maximum local clad oxidation ratio is very small, and is lower than the 15 % limit. Therefore, the acceptance criteria are satisfied. The fuel cladding is not perforated based on the relationship between hoop stress and temperature.

Thus, the effectiveness of the FLSS and RDCF has been demonstrated.

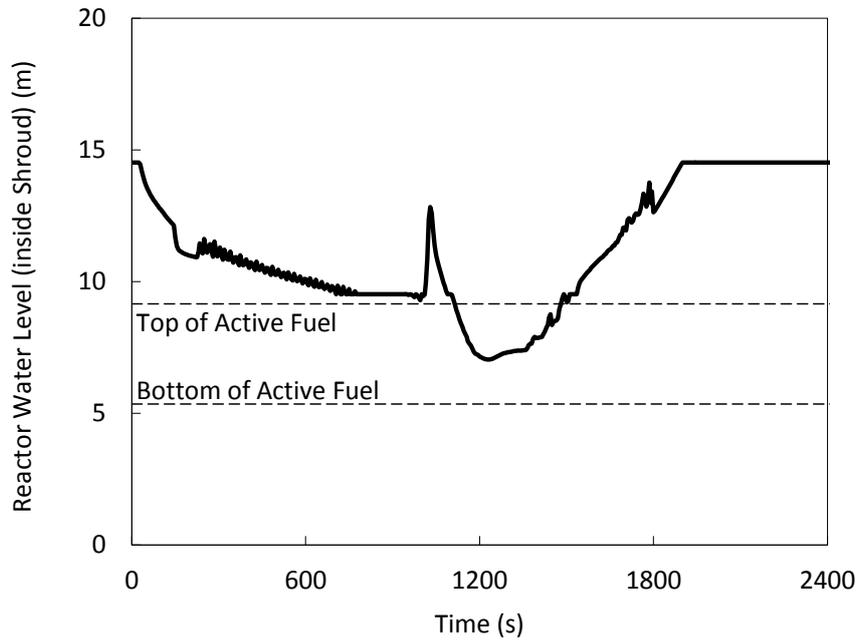
Table 24.12-4: Sequence of Events for Demonstration for Fuel Cooling Function

Time (s)	Events
0	The fault is assumed to start.
Approx. 409	Reactor low water level (Level 1) is reached. FLSS and RDCF receive actuation signals and the delay timer is initiated.
Approx. 1009	RDCF delay timer expires and the RDCF is actuated.
Approx. 1190	Vessel pressure decreases below the FLSS shutoff head. FLSS begins injection.

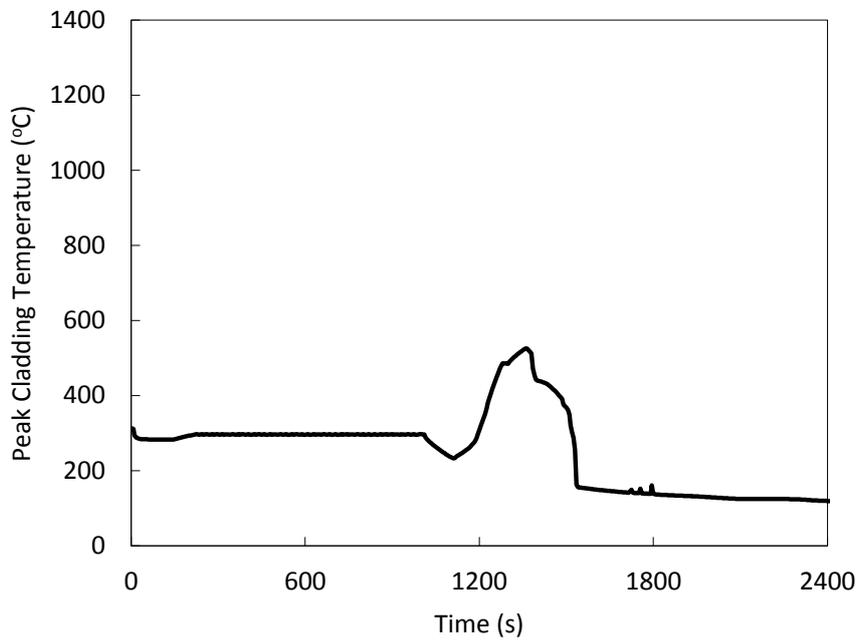


(a) Reactor Pressure

Figure 24.12.1-1: Reactor Pressure Transient for Demonstration of Fuel Cooling Function



(b) Reactor Water Level (inside Shroud)



(c) Peak Cladding Temperature

Figure 24.12.1-1: Reactor Pressure Transient for Demonstration of Fuel Cooling Function (Continued)

(6) Discussion and Conclusions

For each Fundamental Safety Function, the analyses in which the Class 1 systems are unavailable and only Class 2 systems can be used were performed. The effectiveness of the diverse protective means for each Fundamental Safety Function was confirmed.

The results of the analysis of this fault show that all the acceptance criteria are met and those relating to fuel failure are met with a large margin. In addition, only one line of the Class 2 protection systems is claimed in the analysis and there is also the Class 3 FLSR that could be used. The margin on acceptance criteria and the redundancy of protection system make the risk from this fault very low. There are no additional reasonably practicable means of further reducing the risk and the risk is deemed to be ALARP.

24.12.1.3 Demonstration for Long-term Heat Removal Function

Fault Schedule Ref: 2.1.2

(1) Class 1 and Class 2 Systems

Table 24.12-5 shows the Category A Class 1 and Class 2 systems for the Long-term Heat Removal function for frequent faults. Unavailability of all of the RHR heat exchangers is assumed in the analysis and containment venting is used to provide the heat removal function.

Table 24.12-5: A1 and A2 systems for Long-term Heat Removal Function of the Frequent Faults

Category & Class	Safety Systems
A1	<ul style="list-style-type: none"> • RHR - S/P cooling • RHR - LPFL with RHR heat exchanger • RHR - Shutdown cooling • SRV - Manual depressurization
A2	<ul style="list-style-type: none"> • Containment venting

(2) Evaluated Faults

The fault to be evaluated is chosen from the list of frequent faults in terms of the increase of PCV temperature. The analysis for the following fault is performed.

- Inadvertent MSIV closure (Fault Schedule Ref: 2.1)

(3) Acceptance Criteria

The infrequent fault acceptance criteria are used rather than the frequent fault criteria, as the combination of a frequent fault and unavailability of Class 1 SSCs is deemed to be infrequent. The acceptance criteria are given in Section 24.3.3. For this event, which is assessed as an infrequent fault, they are:

AC-C1: Pressure on the primary containment boundary shall be maintained below the maximum allowable working pressure.

AC-D5: Dose to workers should be less than 500 mSv.

AC-D6: Dose to members of the public should be less than 100 mSv.

(4) Analysis Assumptions

The main analysis conditions are shown in Table 24.12-6. Further details of the analysis conditions are described in Attachment H, section H.4.5 of the Topic Report on Design Basis Analysis [Ref-5].

Table 24.12-6: Main Analysis Conditions for Long-term Heat Removal Analysis

No.	Item	Analysis Condition	Remark
1	Reactor thermal power	4005 MW (102% of rated power)	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
2	Blowdown model	N/A	Piping break is not considered.
3	Decay Heat	ANSI/ANS-5.1 decay heat plus 2-sigma	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
4	PCV volume (1) Drywell (2) Suppression Chamber (3) Suppression Pool Water	7350 m ³ 5960 m ³ 3580 m ³	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
5	Initial Pressure (1) Drywell (2) Suppression Chamber	9 kPa [gauge] 9 kPa [gauge]	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
6	Initial Temperature (1) Drywell (2) Suppression Chamber	57 °C 35 °C	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
7	Initial Humidity (1) Drywell (2) Suppression Chamber	20% 100%	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
8	Vent Pipes (1) Flow Area (2) Submergence	11.3 m ² 3.6 m	Same as the long-term PCV performance analysis (shown in Section 24.8.3)
9	Start time of PCV Spray	N/A	PCV spray is not used.
10	RHR heat exchanger capacity	N/A	All of RHR Heat Exchangers are assumed to be failed.
11	RHR heat exchanger Water Supply Temperature	N/A	All of RHR Heat Exchangers are assumed to be failed.
12	Pump Heat	5000 kW	All of ECCS pump heat is considered. [Same as the long-term PCV performance analysis (shown in Section 24.8.3)]
13	Operation of ECCS Water Source	RCIC + FLSS Condensate Storage Tank	
14	Long term heat removal	Containment venting	Containment venting is actuated when PCV pressure reaches 310 kPa [gauge].
15	Vacuum Breaker Actuation pressure	3.4 kPa [dif]	Same as the long-term PCV performance analysis (shown in Section 24.8.3)

(5) Analysis Results

The sequence of events is shown in Table 24.12-7. Analysis results are shown in Figure 24.12.1-2 and Figure 24.12.1-3.

Due to the containment venting, it is demonstrated that the drywell and wetwell pressures are maintained below the containment pressure design limit. It is further concluded that the vent flow is sufficient to control the containment pressures below the design limit.

The peak drywell temperature (159 °C) is also kept below the design value of 171 °C.

The peak temperature reaches 142 °C corresponding to the saturated temperature of the peak PCV pressure. After actuation of containment venting, the suppression pool temperature starts to gradually decrease.

The core and suppression pool are ultimately cooled by the RHR systems when the RHR heat exchangers are recovered.

Table 24.12-7: Sequence of Events for Long-term Heat Removal Analysis

Time	Event
0 second	<ul style="list-style-type: none"> •MSIVs close instantaneously • Reactor Scram occurs. •Motor Driven Feedwater pumps maintain feedwater injection
Approx. 3.2 hours	<ul style="list-style-type: none"> •FW is depleted. HPCF and RCIC are made available to maintain the RPV water level between Level 1.5 and Level 8. (RCIC does not initiate because the vessel water level does not drop below Level 1.5 until after the RPV pressure falls below 150 psig.)
4 hours	<ul style="list-style-type: none"> •Operator starts to depressurize the RPV and the RPV depressurisation rate is assumed to be 55 °C/h.
Approx. 5.7 hours	<ul style="list-style-type: none"> •RPV pressure is below the pressure permissive for FLSS injection and the FLSS maintains reactor water level between Level 3 and Level 8.
Approx. 10.9 hours	<ul style="list-style-type: none"> •PCV pressure reaches 310 kPa [gauge]. •Containment venting is initiated.

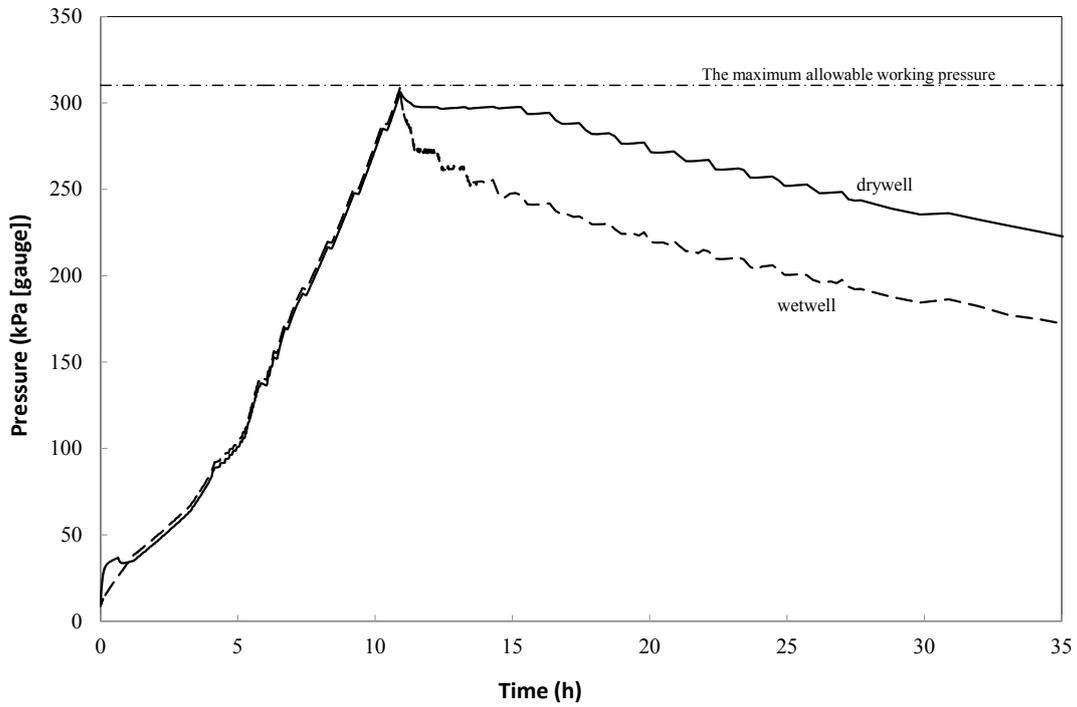


Figure 24.12.1-2: Pressures Transients in the Drywell and Wetwell

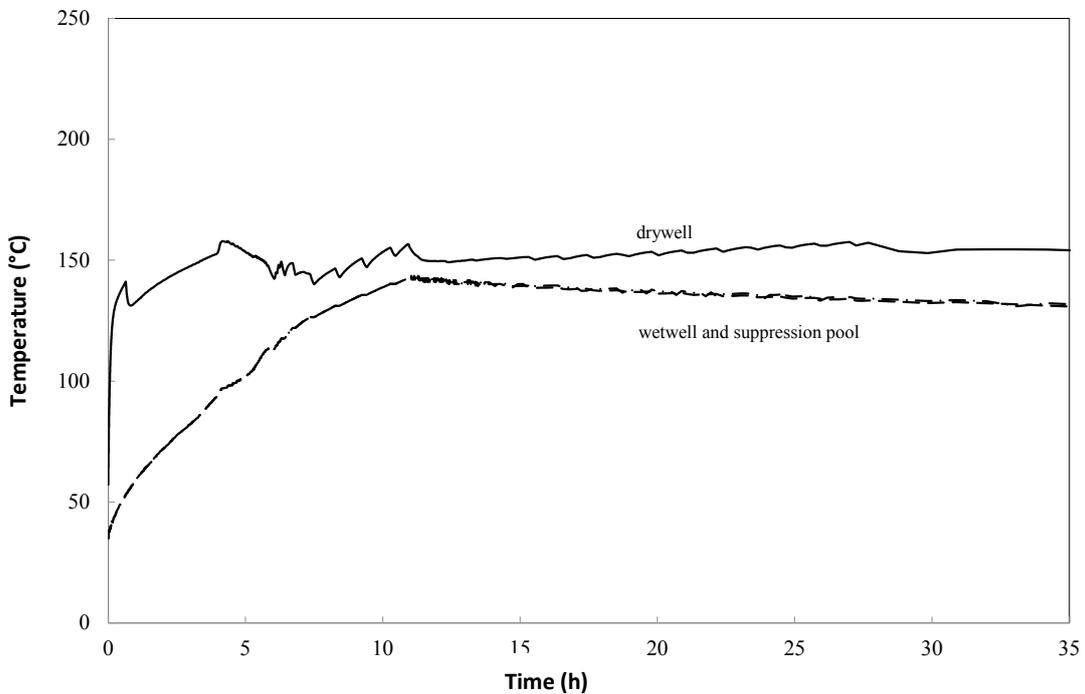


Figure 24.12.1-3: Temperature Transients in the Drywell, Wetwell and Suppression Pool

(6) Discussion and Conclusions

For each Fundamental Safety Function, the analyses in which the Class 1 systems are unavailable and only Class 2 systems can be used were performed. The effectiveness of the diverse protective means for each Fundamental Safety Function was confirmed.

The results of the analysis of this fault show that all the acceptance criteria are met and those relating to PCV temperature are met with a margin. In addition, only one line of the Class 2 protection systems is claimed in the analysis. The margin on acceptance criteria and the redundancy of protection system make the risk from this fault very low. There are no additional reasonably practicable means of further reducing the risk and the risk is deemed to be ALARP.

24.13 Post-Accident Management for Safe Shutdown Following Design Basis Faults

The analyses presented in Sections 24.6 to 24.9 show that the UK ABWR can be brought to a hot shutdown state following Design Basis Reactor Faults. The following subsections describe post-accident management procedures for taking the plant to a cold shutdown state following each reactor fault type.

24.13.1 Normal shutdown

The process to bring the reactor to cold shutdown conditions from normal power operation is as follows:

- (1) The RIPs are run back to reduce flow and the control rods then begin to be inserted to reduce the reactor power.
- (2) Once the electrical power reaches about 10%, the turbine is tripped and steam bypassed to the main condenser. Cooling is maintained by feedwater flow and steam bypass. After that, all the control rods are inserted.
- (3) The reactor pressure is decreased by the steam being blown down to the main condenser.
- (4) When the reactor pressure reduces less than about 0.93 MPa[gage], the feedwater is tripped and RHR started in shutdown cooling mode. At this point, the condenser vacuum is also lost.
- (5) Operation of the RHR brings the reactor to shutdown conditions: the reactor coolant temperature < 100°C

The RHR is a Class 1 system but all the other functions required during the shutdown process are Class 3.

24.13.2 Non-Isolation Events

If a non-isolation event occurs, the response to the transient is for the RCS to trip the reactor but, otherwise, reactor is in essentially the same configuration as for normal shutdown. In particular, the MSIVs are not closed and cooling by feedwater and turbine bypass can be initiated as for normal shutdown. Non-isolation events fall into three broad groups:

- (1) Events with reduced core flow (Loss of RIPs)

In these events, trip of some or all RIPs leads to the control rods being inserted by RCS - the progression essentially follows the normal shutdown process (run-back of RIPs followed by rod insertion) even though the timing may be different and the events less controlled. Feedwater is available and the reactor is brought to cold shutdown by essentially the same process as for normal shutdown.

(2) Events with feedwater faults but not loss of feedwater (failure of controller or feed heaters)

In these events, feedwater is faulted but still available and, although the reactor is tripped earlier in the process than for normal shutdown, the shutdown process continues essentially in the same way as for normal shutdown.

(3) Events with control rod faults

In these cases, the power at the start of the transient deviates from normal power. The response of the protection system is to trip the reactor and the RIPs. Since feedwater is available, again the reactor is essentially in the same state as for normal shutdown, albeit with different timescales.

In all cases, even if the primary circuit pressure has been transiently increased, cooling by feedwater and turbine bypass brings the primary pressure down to the point where RHR can be initiated to achieve cold shutdown as in the normal case.

24.13.3 Isolation Events

The main feature of isolation events is that the MSIVs are closed. This means that cooling by feedwater and turbine bypass is not possible. The RCS trips the reactor bringing it to a hot shutdown condition but then the philosophy for cooling the reactor and bringing the reactor to cold shutdown conditions is as follows:

(1) Water level is maintained initially by actuation of RCIC on low water level (L1.5) after reactor trip, supported by HPCF if necessary, although only one division of RCIC/HPCF is required to fulfil this function.

(2) Excess steam is vented from the reactor coolant circuit by passive operation of the SRVs to the S/P and heat is removed using the RHR suppression pool cooling mode once the S/P temperature exceeds 49°C.

(3) Once the reactor coolant circuit pressure reaches 1.6 MPa [gage], water RCIC and HPCF are replaced by initiation of RHR [LPFL mode]. Only one division of RHR is required to fulfil this function.

(4) If the SRVs close, depressurisation of the reactor continues by manual actuation of the SRVs

(5) RHR (LPFL mode) is switched over to RHR (shutdown cooling) after core water level is recovered and reactor pressure gets below approx.0.93MPa [gage].

The SSCs that provide HLSFs in the case of isolation events are listed in Table 24.7-1. For all isolation events these SSCs are powered by the essential electrical supply buses. In the case of LOOP events, these buses receive power from the EDGs rather than off-site power.

Figure 24.13-1 shows the base-case analysis for shutdown following an isolation event from Attachment G of the Topic Report on Design Basis Analysis [Ref-5].

Attachment G of [Ref-5] also discusses a number of cases other than the base case to demonstrate that all isolation events can be brought to cold shutdown conditions.

24.13.4 Loss of Cooling Events

In the event of a LOCA inside containment, the Reactor Protection System (RPS) trips the reactor and closes the MSIVs to maintain coolant inventory. Following this, RHR heat exchanger is activated automatically to remove heat with the RCW System and ultimately to the RSW System. As presented in Section 24.8.3, the PCV can be cooled under the conservative assumption that only one train of RHR is available. In this case, since PCV is cooled by overflow of ECCS water from the RPV (via broken piping), both core and PCV can be cooled without any operator action.

For LOCAs outside containment, after the primary containment isolation by the isolation valves closure, these events also follow the same procedure as for isolation events.

The SSCs providing HLSFs for LOCA events are shown in Table 24.8-1.

24.13.5 ATWS Events

An ATWS event is either a non-isolation event or an isolation event with failure of the reactor to trip. The first response in these cases is for the HWBS to try to insert the control rods using ARI. If this is successful, the reactor trips quickly and the case is just as the corresponding event described above and the reactor is brought to cold shutdown conditions as for those cases.

If the actuation of ARI is unsuccessful, HWBS brings the reactor to hot shutdown by automatic boron injection by actuating SLC. Control rods are then driven in by the Class 3 RCIS using the control rod follow in function or manually after recovery of the control rod drive system. If control rods can be inserted, the resulting state is the same as the corresponding non-isolation or isolation fault and is brought to cold shutdown accordingly. However, if recovery of control rod cannot be

achieved, the reactor is depressurised by opening SRVs manually until the pressure is low enough for RHR shutdown cooling mode can be activated. The reactor water level during this period is maintained by using HPCF, LPFL or FLSS. The reactor is brought to safe shutdown state by RHR reactor shutdown cooling mode as in other cases.

The SSCs providing HLSFs for ATWS events are shown in Table 24.9-1.

24.13.6 SBO Events

If Medium term SBO occurs, the operators depressurise the RPV within 8 hours and cooling water is injected into the RPV using the low pressure injection system (FLSS or FLSSR) after manual depressurisation. Following this, heat removal is implemented by containment venting when the PCV pressure reaches its design pressure. The suppression pool is cooled by the RHR system in S/P cooling mode after recovery of off-site power. Subsequently, when the S/P temperature decreases below 100 °C, the reactor is brought to cold shutdown by RHR realignment by the operators to switchover from RHR S/P cooling mode to reactor shutdown cooling mode.

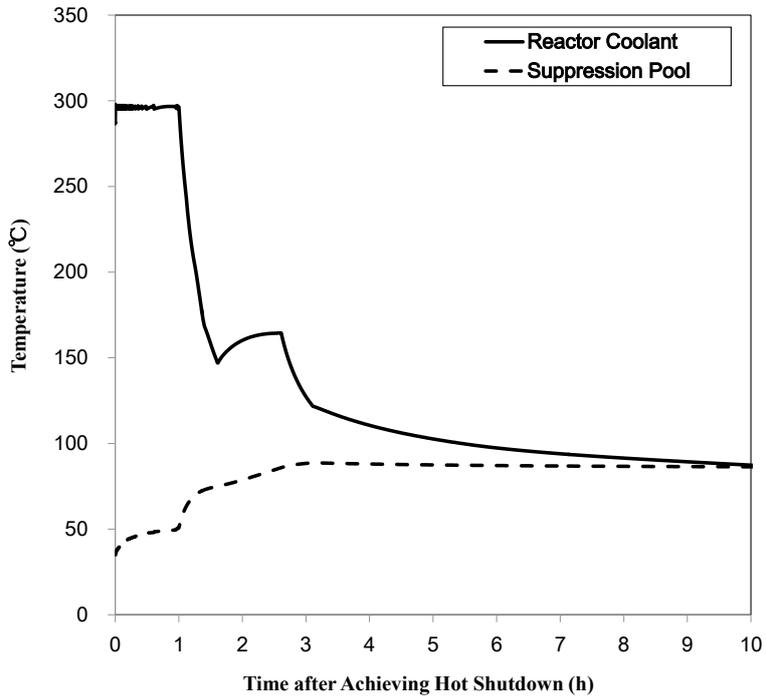


Figure 24.13-1: Shutdown following an Isolation Event

24.14 Assumptions, Limits and Conditions for Operation

Limits and Conditions for Operation are defined throughout the chapter and are listed at the beginning of each fault group along with the Analysis Conditions and Provision of HLSFs.

24.15 Summary of ALARP Justification

This section presents a high level overview of how the ALARP principle has been applied for the design basis analysis, and how this contributes to the overall ALARP argument for the UK ABWR.

Chapter 28 of this PCSR (ALARP Evaluation) presents the high level approach taken for demonstrating ALARP across all aspects of the design and operation. It presents an overview of how the UK ABWR design has evolved, the further options that have been considered across all technical areas resulting in a number of design changes, and how these contribute to the overall ALARP case. The approach to undertaking ALARP Assessment during GDA is described in the GDA ALARP Methodology [Ref-22] and Safety Case Development Manual [Ref-23].

Each of the systems chapters of the PCSR includes a ‘Summary of ALARP Justification’ section which lists the most significant nuclear safety risks associated with the SSCs within the scope of the chapter. Those sections then go on to describe various ALARP evaluations that have been performed for those SSCs. The ALARP evaluations include risk assessments against the risk targets specified in the NSEDPs [Ref-24], and generally take account of nuclear safety, conventional safety and environmental safety. Specifically, the nuclear safety risk assessments include the following:

- (i) Failure Modes and Effects Analysis (FMEA) of the Systems
- (ii) Deterministic Safety Analysis – consisting of Design Basis Analysis, Beyond Design Basis Analysis (BDBA) , and Severe Accident Analysis (SAA)
- (iii) Probabilistic Safety Analysis
- (iv) Wide-ranging Human Factors Analysis
- (v) Worker Dose assessments during normal operation and faults

For more details of these risk assessments, see the example for the ECCS in Section 7 of BSC on ECCS [Ref-25].

The general conclusion from the system chapters is that in the context of GDA, the risks associated with the provision of the HLSFs required to protect the reactor and other sources of radioactivity from faults are ALARP.

The assessments presented in this chapter cover the full range of Design Basis risks but do not consider any additional nuclear safety risks for specific systems that are not already listed elsewhere in the PCSR. However, the Design Basis Analysis is a crucial part of the demonstration that those risks are ALARP. Each individual fault analysed in this chapter only addresses a subset of the total set of risks that are listed within the ALARP sections of the systems chapters. However every one of

the full set of risks that is relevant to design basis fault conditions is bounded by at least one of the design basis faults that are described in this chapter.

Good practice in the design of systems that are important to the protection of the plant against design basis faults is considered elsewhere in the ALARP sections of the PCSR chapters that describe those systems. The methodology used for the design basis analysis itself follows good practice, as described elsewhere in this chapter, including such things as:

- Application of conservative assumptions, including the single failure criterion described in Safety Case Development Manual [Ref-23].
- Credit is not taken for correct performance of control systems where this would increase margins to the analysis acceptance criteria.
- All acceptance criteria (including dose) are met just claiming the A1 systems.
- Correct performance of control systems is assumed if this exacerbates the fault conditions.
- Use of computer codes that have been validated for use for analysis of the types of fault conditions that are being assessed.
- Application of acceptance criteria that are based on high quality experimental data and extensive worldwide operating experience.
- Identification of limits and conditions for operation to ensure that the performance of the actual operating plant always remains bounded by the assumptions made in the design basis analysis (Section 24.14).
- The analysis of each design basis fault considers the most onerous operating mode of the plant for that particular fault.
- Diverse protection by Class 2 systems is demonstrated to be effective for all frequent faults.

For most faults involving the reactor except for LOCAs, it is concluded that at all three barriers to release of radioactivity (fuel cladding, reactor coolant pressure boundary and primary containment) remain intact and that there are no radiological consequences. In the case of LOCAs, the reactor coolant pressure boundary is not intact but, in all cases, fuel integrity is preserved. However, in some cases, there is release to the environment as the containment function may also be bypassed. Even in these cases the dose criteria are met. In most cases, there is significant margin before fuel cladding, reactor coolant boundary and containment acceptance criteria are threatened.

However, there are some design basis faults where the margin to failure of one of the barriers has been able to be improved in reasonably practicable ways.

For example, the margin to the primary containment boundary limits in some of the more extreme Loss of Off-site Power events (LOOP with CCF of EDGs) can be improved if alternative AC power could be made available. This event is part of the consideration that led to the adoption of the Diverse Additional Generator (DAG) into the design of UK ABWR for GDA, as described in PCSR Chapter 15.

Another example is the increase in sizing of the RHR heat exchangers in UK ABWR to provide full N+2 redundancy for the RHR system. This increases the reliability of long term heat removal for DB faults and also decreases the frequency of loss of heat removal faults during shutdown.

A third, related, example is the redesign of FPC to make it Class 1 to reduce the frequency of loss of heat removal faults in SFP.

The analysis performed to demonstrate that Design Basis Acceptance Criteria are met uses very conservative assumptions with no credit being taken for any Class 2 or Class 3 systems that are available to provide the same HLSFs as the claimed Class 1 systems, although there is a demonstration that Class 2 systems can bring the reactor to safe shutdown conditions for frequent faults in the case that Class 1 systems are not available. However, in practice, there are a number of Class 2 or Class 3 systems that would be available in the event of a fault. In fact, in many cases, the operation of these systems would be the normal plant response with the Class 1 systems acting as a backup. In this way, the design has considerable defence in depth over and above the margins on acceptance criteria.

This chapter of the PCSR has demonstrated that:

- there is considerable defence in depth and diversity in the design;
- the margins to acceptance criteria not being met are often significant;
- in all Design Basis faults, there is at least one barrier remaining to prevent radioactive releases in excess of dose acceptance criteria;

in addition to the demonstrations in other chapters that there are no further reasonably practicable ways to improve the provision of HLSFs claimed in the Design Basis assessment. The conclusion is that, as far as Design Basis faults are concerned, the risk from UK ABWR is ALARP.

24.16 Conclusions

The analysis for frequent and infrequent design basis faults including a range of common cause initiators, support system failures, SFP and fuel route faults and other non-reactor faults for the UK ABWR has been performed. As shown in the “Analysis Results and Fault-based View” sub-sections of this chapter, all acceptance criteria for frequent and infrequent design basis faults are met. Therefore, the adequacy of the safety design and the suitability and sufficiency of the safety measures for the base set of initiating events are confirmed against DB targets in the NSEDPs.

The analysis reported in the chapter is performed on the basis of a number of conservative assumptions listed in 24.5.2 and assumes that the SSCs providing HLSFs satisfy the SFCs and SPCs associated with them and discussed in the engineering chapters.

The chapter demonstrates that, even with conservative assumptions, the conservative acceptance criteria are met giving confidence of the adequacy of the defence-in-depth and diversity in the design and that the design is therefore fault tolerant to faults. The risk from each individual bounding fault assessed in this chapter is shown to be ALARP leading to the conclusion that overall risks from Design Basis faults are ALARP.

24.17 References

- [Ref-1] IAEA, "IAEA SAFETY STANDARDS SERIES -Safety Assessment and Verification for Nuclear Power Plants", NS-G-1.2, 2001.
- [Ref-2] GE Nuclear Energy, "ABWR Design Control Document", 1997.
- [Ref-3] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Fault Assessment", GA91-9201-0001-00022 (UE-GD-0071) Rev.6, July 2017.
- [Ref-4] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Fault Assessment for SFP and Fuel Route", GA91-9201-0001-00082 (AE-GD-0229) Rev.3, July 2017.
- [Ref-5] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Design Basis Analysis", GA91-9201-0001-00023 (UE-GD-0219) Rev.14, August 2017.
- [Ref-6] Hitachi-GE Nuclear Energy, Ltd., "Description of ODYN/STEMP Code", GA91-9201-0003-00139 (3E-GD-D054) Rev.0, August 2014.
- [Ref-7] Hitachi-GE Nuclear Energy, Ltd., "Description of ISOCCR Code", GA91-9201-0003-00140 (UE-GD-0213) Rev.0, August 2014.
- [Ref-8] Hitachi-GE Nuclear Energy, Ltd., "Description of TASC Code", GA91-9201-0003-00141 (UE-GD-0217) Rev.0, August 2014.
- [Ref-9] Hitachi-GE Nuclear Energy, Ltd., "Description of Lattice Analysis Code and 3-D Core Simulator", GA91-9201-0003-00003 (UE-GD-0093) Rev.2, October 2016.
- [Ref-10] Hitachi-GE Nuclear Energy, Ltd., "Description of TRACG Code", GA91-9201-0003-00146 (UE-GD-0218) Rev.0, August 2014.
- [Ref-11] Hitachi-GE Nuclear Energy, Ltd., "Description of LAMB Code", GA91-9201-0003-00142 (AE-GD-0182) Rev.0, August 2014.
- [Ref-12] Hitachi-GE Nuclear Energy, Ltd., "Description of SAFER Code", GA91-9201-0003-00143 (AE-GD-0183) Rev.0, August 2014.
- [Ref-13] Hitachi-GE Nuclear Energy, Ltd., "Description of PCV Analysis Code", GA91-9201-0003-00144 (ASE-GD-0014) Rev.0, August 2014.
- [Ref-14] Hitachi-GE Nuclear Energy, Ltd., "Description of RADTRAD Code", GA91-9201-0003-00145 (HE-GD-0051) Rev.0, August 2014.
- [Ref-15] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Design Basis Analysis for SFP and Fuel Route", GA91-9201-0001-00137 (AE-GD-0441) Rev.3, June 2017.
- [Ref-16] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on SBO Analysis", GA91-9201-0001-00114 (AE-GD-0265) Rev.7, June, 2017.
- [Ref-17] Hitachi-GE Nuclear Energy, Ltd., "A Study of Chemistry Effects in UK ABWR Fault Studies", GA91-9201-0003-01330 (HE-GD-0175) Rev.2, July 2017.
- [Ref-18] Hitachi-GE Nuclear Energy, Ltd., "DBA radiological consequence – analysis assumptions (Response to RQ-ABWR-0411)", GA91-9201-0003-00748 (HE-GD-0086) Rev.0, May 2015.
- [Ref-19] MCNP - A General Monte Carlo N-Particle Transport Code, Version 5, Volume I: Overview and Theory, LA-UR-03-1987, February 2008
- [Ref-20] The QAD section of "Gamma Rays Shielding Design Handbook", Atomic Energy Society of Japan, January 1988.
- [Ref-21] NRC, "Calculation of Distance Factors for Power and Test Reactor Sites", TID-14844 (1962)
- [Ref-22] Hitachi-GE Nuclear Energy, Ltd., "GDA ALARP Methodology", GA10-0511-0004-00001 (XD-GD-0037) Rev 1, November 2015.

- [Ref-23] Hitachi-GE Nuclear Energy, Ltd., “GDA Safety Case Development Manual”, GA10-0511-0006-00001 (XD-GD-0036) Rev. 3, June. 2017.
- [Ref-24] Hitachi-GE Nuclear Energy, Ltd., “UK ABWR Nuclear Safety and Environmental Design Principles (NSEDPs)”, GA10-0511-0011-00001 (XD-GD-0046) Rev 1, July 2017.
- [Ref-25] Hitachi-GE Nuclear Energy, Ltd., “Basis of Safety Cases on Emergency Core Cooling systems”, GA91-9201-0002-00020 (SE-GD-0164) Rev 2, June 2017.
- [Ref-26] Hitachi-GE Nuclear Energy, Ltd., “Standard Control Procedure for Identification and Registration of Assumptions, Limits and Condition for Operation”, GA91-0512-0010-00001, Rev 1, November 2016.
- [Ref-27] Hitachi-GE Nuclear Energy, Ltd.,” Generic Technical Specifications”, GA80-1502-0002-00001, Rev 3, August 2017.
- [Ref-28] Hitachi-GE Nuclear Energy, Ltd., “Containment Performance Analysis Report in UK ABWR”, GA91-9201-0003-00985 (AE-GD-0561) Rev.3, June 2017
- [Ref-29] Hitachi-GE Nuclear Energy, Ltd., “Calculation of Primary Source Term Value”, GA91-9201-0003-00928 (WPE-GD-0196) Rev.3, Jun 2016
- [Ref-30] US NRC, Light Water Reactor Hydrogen Manual”, NUREG/CR-2726, June 1983.
- [Ref-31] K R Smith and A L Jones, “Generalised Habit Data for Radiological Assessments“, NRPB-W41, 2003.
- [Ref-32] ICRP, “Age-dependent Doses to Members of the Public from Intake of Radionuclides - Part 4 Inhalation Dose Coefficients”, ICRP Publication 71, Ann. ICRP 25 (3-4), 1995
- [Ref-33] K F Eckerman and J C Ryman, “External Exposure to Radionuclides in Air, Water and Soil”, Federal Guidance Report 12. EPA Report 402-R-93-081. Washington, DC, 1993.
- [Ref-34] Hitachi-GE Nuclear Energy, Ltd., “Overarching report on support systems safety case”, GA91-9201-0003-02059 (UE-GD-0688) Rev.1, May 2017.
- [Ref-35] Hitachi-GE Nuclear Energy, Ltd., “Topic Report on ALARP Assessment for Steam Generation resulting from a Loss of Decay Heat Removal from the SFP and pen RPV”, GA91-9201-0001-00274 (AE-GD-0989) Rev.0, May 2017.
- [Ref-36] Hitachi-GE Nuclear Energy, Ltd., “Topic Report on ALARP Assessment for Off-Gas System” GA91-9201-0001-00125 (GE-GD-0035) Rev.4, July 2017.
- [Ref-37] Hitachi-GE Nuclear Energy, Ltd., “Reliability of Canister Integrity for Cask Drops”, GA91-9201-0003-00917 (FRE-GD-0086) Rev.3 November 2016
- [Ref-38] Hitachi-GE Nuclear Energy, Ltd., “ALARP Assessment Report for Fuel Route”, GA91-9201-0003-00814 (AE-GD-0472) Rev.1, June 2017
- [Ref-40] Hitachi-GE Nuclear Energy, Ltd., “Topic Report on Cask Drop Frequency”, GA91-9201-0001-00201 (M1E-UK-0062) Rev.1, April 2016.
- [Ref-41] Hitachi-GE Nuclear Energy, Ltd., “Feasibility of Impact Limiters for Cask Drops”, GA91-9201-0003-00436 (FRE-GD-0041) Rev.5, November 2016.
- [Ref-42] Hitachi-GE Nuclear Energy, Ltd., “Spent Fuel Interim Storage Optioneering for Spent Fuel Removal from Spent Fuel Pool to Outside of Reactor Building”, GA91-9201-0003-00689 (FRE-GD-0080) Rev.3, September 2016.
- [Ref-43] Hitachi-GE Nuclear Energy, Ltd., “ALARP Report for Spent Fuel Export”, GA91-9201-0003-01563 (FRE-GD-0144) Rev.0, September 2016.

Appendix A Table of SFC Claims

Chapter 24 does not introduce any SFCs but relies on SFCs in other chapters. This Appendix shows the relationship between the DBA presented in this chapter and the Safety Functional Claims (SFCs) used elsewhere in the PCSR.

The DB analysis presented in this chapter demonstrates that the principal barriers to radiological releases (fuel cladding, reactor coolant circuit pressure boundary and containment) are not compromised in any DB fault. In order to demonstrate this, faults are analysed against a set of Acceptance Criteria derived from SFCs in other parts of the PCSR. These Acceptance Criteria reflect the claimed withstand capability of the principal barriers in terms of parameters modelled in the transient analysis. Simply put, if the transient analysis shows that the relevant parameter is within the limits expressed in the SFC and incorporated in the corresponding Acceptance Criteria, then the corresponding barrier failure mechanism will not occur, that is, the transient analysis forms the evidence that substantiates the corresponding claim.

The Acceptance Criteria and the corresponding SFCs are shown in Table A-1.

Table A-1 SFCs from which Fault Studies Acceptance Criteria are derived

Acceptance Criteria		SFC	
AC-F1	The critical power ratio (CPR) shall be greater than the safety limit minimum CPR (MCPR), so as to maintain nucleate boiling	THD SFC 2-1.1 (11)*	At normal operation and frequent design basis faults, MCPR is equal to or has margin to the safety limit so as to preclude thermal failure with overheating.
AC-F2	Fuel cladding shall not be mechanically damaged. That is, the surface heat flux of the fuel cladding shall not exceed the Thermal Over-Power (TOP) or the Mechanical Over-Power (MOP) limits.	FA SFC 4-10.3 (11)	The cladding circumferential strain due to pellet-clad mechanical interaction is less than the design limit at normal operation and all frequent design basis faults so as to preclude mechanical failure due to cladding strain.
AC-F3	The calculated maximum fuel cladding temperature shall not exceed 800°C or the ballooning rupture (perforation) temperature, so as to preclude cladding failure.	THD SFC 2-1.2 (11)	At normal operation and frequent design basis faults, when MCPR becomes less than the safety limit, cladding temperature is less than 800 °C such that ballooning rupture failure is precluded.
AC-F4	The calculated total oxidation of the fuel cladding shall not exceed 15% of the total cladding thickness before oxidation.	FA SFC 2-1.2 (11)	In all infrequent design basis faults, peak cladding oxidation is less than 15 percent equivalent cladding reacted (ECR).
AC-F5	The calculated maximum fuel cladding temperature shall not exceed 1200°C	FA SFC 2-1.1 (11)	In all infrequent design basis faults, peak cladding temperature is less than 1,200 °C .
AC-F6	Fuel enthalpy shall not exceed the design limit in the case of a reactivity insertion fault.	FA SFC 2-1.3 (11)	Fuel enthalpy meets the prescribed design limit for all frequent and infrequent design basis faults.

Table A-1 SFCs from which Fault Studies Acceptance Criteria are derived

Acceptance Criteria		SFC	
AC-F7	Fuel enthalpy shall not exceed the limit value to prevent the generation of mechanical energy in the case of reactivity insertion faults.	FA SFC 2-1.3 (11)	Fuel enthalpy meets the prescribed design limit for all frequent and infrequent design basis faults.
AC-R1	Pressure on the reactor coolant pressure boundary shall be maintained below 110% of the maximum allowable working pressure (applies to frequent faults)	NB SFC 4-2.1 (12)	The MS through the safety valve function of the SRVs is the principal means to deliver overpressure protection of the RCPB under abnormal transients and accident conditions that could put excessive pressure on the boundary.
AC-R2	Pressure on the reactor coolant pressure boundary shall be maintained below 120% of the maximum allowable working pressure (applies to infrequent faults)		
AC-C1	Pressure and Temperature on the primary containment boundary shall be maintained below the maximum design pressure and temperature	PCV SFC 4-7.2 (13)	The RCCV is designed so that it can withstand maximum design pressure and maximum design temperature produced as a result of any hypothetical LOCA, including an instantaneous complete break of one feedwater line, which is the limiting LOCA pipe break from a containment integrity perspective.
AC-N1	k_{eff} shall be smaller than 0.95 to maintain sub-criticality in the SFP	SFS SFC 1-9.1 (19)	The spent fuel storage racks maintain the Fuel Assemblies in a subcritical state.
AC-W1	Reactor Pressure Vessel (RPV) water level shall be maintained above the Top of Active Fuel (TAF) of the reactor core during	SFS SFC 2-4.1 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.

Table A-1 SFCs from which Fault Studies Acceptance Criteria are derived

Acceptance Criteria		SFC	
	shutdown to prevent the fuel being uncovered and heating up.	SFS SFC 4-7.1 (19)	The SFP, the Cask Pit, and associated SFP gates are designed to prevent loss of SFP water.
		SFS SFC 4-7.2 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.
AC-W2	SFP water level shall be maintained above the TAF of the spent fuel pool to prevent spent fuel being uncovered and heating up	SFS SFC 2-4.1 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.
		SFS SFC 4-7.1 (19)	The SFP, the Cask Pit, and associated SFP gates are designed to prevent loss of SFP water.
		SFS SFC 4-7.2 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.
AC-C2	Canister deceleration following a design basis drop shall remain below allowable limit	SFE SFC 4-14.1 (19)	Containment function will be maintained during SFE unsealed canister operations and associated fault conditions.
		SFE SFC 4-14.2	Containment function will be maintained during SFE sealed canister operations and associated fault conditions.

* The number in brackets shows the PCSR chapter where the SFC is claimed. The description of the SFCs can be found in Appendix A of the corresponding chapter.

NOT PROTECTIVELY MARKED

Form05/01

UK ABWR

Generic Pre-Construction Safety Report

Revision C

For most DB faults, the Acceptance Criteria ensure that barriers remain intact. These Acceptance Criteria therefore constitute assumptions and LCOs that maintain doses within limits. However, there are a small number of faults where other criteria also need to be met. For example, the dose may only be limited if a specific radioactive inventory is kept within the corresponding limit. For these faults, there is a LCO identified (or implied) that requires sampling and monitoring of reactor coolant, SFP or radioactive waste systems to ensure that the limit is not exceeded in operation, related to the following SFC:

LCO	SFC	
Activity levels in Reactor Coolant, SFP or Radioactive Waste Systems	RC SC 13.1 (see PCSR Section 23.10.2)	The chemistry sampling and monitoring system provides the analytical information of each SSCs associated with an Operating Rule

In order to demonstrate that Acceptance Criteria are met in the (protected) DB case, the transient analysis assumes the availability of the protective and mitigative safety systems that make up the UK ABWR design. Other chapters of the PCSR specify SFCs for each of these safety systems that are claimed in the fault schedule to fulfil specific High Level Safety Functions (HLSFs) (see Chapter 5 Table5.6-1) and used in the transient analysis for each of the bounding design basis faults.

The key SFCs claimed for the principal safety systems are shown in Table A-2, which also shows where in the PCSR the system is described. The SFCs are substantiated in the corresponding Basis of Safety Case (BSC), which is referenced in the corresponding chapter.

The analysis of infrequent faults relies on the provision of Class 1 SSCs. Frequent faults also rely on the provision of Class 2 SSCs.

Table A-2 SFCs relating to safety systems claimed in Fault Studies

Reactivity Control - Reactor			SFCs	
Class 1	HLSF 1-3	Control rod and control rod drive system (CRD) (see Section 11.5.2, 12.4.3.1)	CRD SFC 1-3.1 (12)*	The CRD is the principal means to provide reactor rapid shutdown under RPS signal in conjunction with the CRs by performing CRs insertion, (actuation known as Scram), so that fuel design margins are not exceeded in the event of frequent faults and infrequent faults requiring reactor shutdown.
Class 2	HLSF 1-5	Standby Liquid Control System (SLC) (see Section 11.5.3 and 12.4.3.2)	SLC SFC 1-5.1 (12)	The SLC is the secondary means to provide reactor shutdown without CRs insertion, from full power operation, even during cycle equilibrium, to cold sub-critical condition by injecting the neutron absorbing solution into the reactor core in the event of Anticipated Transient Without Scram (ATWS) design basis fault.
		Alternative Rod Insertion (ARI) (see Section 12.4.3.1)	CRD SFC 1-5.1 (12)	The CRD portions operated under the ARI signal are part of the secondary means to provide alternative reactor shutdown in the event of a frequent fault where reactor shutdown by Scram has failed (event known as ATWS).

* The number in brackets shows the PCSR chapter where the SFC is claimed. The description of the SFCs can be found in Appendix A of the corresponding chapter.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Reactivity Control - Reactor			SFCs	
Class 2	HLSF 1-5	Recirculation Pump Trip (RPT) (see Section 14.6.3)	RRS SFC 1-5.1 (12)	The RIPs of the RRS are tripped by the RPT by a signal from the Hardwired Backup System (HWBS) as part of the actions to perform alternative shutdown of the reactor in the event of ATWS.
		Feed water Stop (see see Section 14.6.3)	NB SFC 1-5.1 (12)	The FDW flow is controlled by the Hardwired Back-up System logic in order to prevent reactivity insertion in the event of ATWS.
Fuel Cooling – Reactor			SFCs	
Class 1	HLSF 2-1	Reactor Core Isolation Cooling System (RCIC) (see Section 13.4.1)	RCIC SFC 2-1.1 (13)	The RCIC is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in high pressure state and in the interval it is being depressurised so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of frequent faults such as loss of the normal feedwater supply and infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 1	HLSF 2-1	Reactor Core Isolation Cooling System (RCIC) (see Section 13.4.1)	RCIC SFC 2-1.2 (13)	The RCIC is capable of providing reactor core cooling during at least 8 hours so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of Loss of Offsite Power Supply (LOOP) and loss of all the AC emergency power sources.
		High Pressure Core Flooder System (HPCF) (see Section 13.4.1)	HPCF SFC 2-1.1 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in high pressure state and in the interval it is being depressurised so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of frequent faults such as loss of the normal feedwater supply and infrequent faults such as LOCA.
			HPCF SFC 2-1.2 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 1	HLSF 2-1	Low Pressure Core Flooder System (LPFL) (see Section 13.4.1)	RHR SFC 2-1.1 (12, 13)	The LPFL is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.
		Safety Relief Valve (SRV) -Safety valve function- (see Section 12.3.3)	NB SFC 2-1.1 (12)	The MS through the safety valve function of the SRV is the principal means to release the steam generated during reactor core cooling by high pressure core cooling systems in the event of faults such as LOCA outside the PCV.
		Automatic Depressurisation System (ADS) (see Section 12.3.3, 13.4.1)	NB SFC 2-1.3 (12, 13)	The NB through the ADS is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA inside the PCV.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 1	HLSF 2-1	Transient Automatic Depressurisation System (Transient ADS) (see Section 12.3.3, 13.4.1)	NB SFC 2-1.4 (12, 13)	The NB through the transient ADS is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA outside the PCV.
Class 2	HLSF 2-2	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-2.1 (13, 16)	The FLSS is the secondary means to provide reactor core cooling in order to prevent significant damage to the fuel and minimise the reaction between the fuel cladding and the reactor coolant sufficiently so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of design basis faults with all the primary reactor core cooling means (ECCS) have failed.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 2	HLSF 2-2	Reactor Depressurisation Control Facility (RDCF) (Alternative SRV) (see Section 16.7.3.3)	RDCF SFC 2-2.1 (13, 16)	The RDCF is an alternative means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults where the primary means (ECCS) are not available.
			RDCF SFC 2-2.2 (13, 16)	The RDCF is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS after RCIC operation for the first 24 hours in the event of design basis faults such as SBO or Class 1 CCF.
Class 3	HLSF 2-2	Reactor Depressurisation Control Facility (Switching Valve for SRV) (RDCF) (see Section 16.7.3.3)	RDCF SFC 2-2.3 (13, 16)	The RDCF with switching valves is the principal means to maintain RPV depressurisation in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults such as SBO or Class 1 CCF after the first 24 hours.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Long Term Heat Removal- Reactor			SFCs	
Class 1	HLSF 3-1	Safety Relief Valve (SRV) –Manual depressurisation– (see Section 12.3.5.2)	NB SFC 3-1.1 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal to reach reactor cold shutdown by depressurisation of the RPV in the event of unavailability of the main condenser.
			NB SFC 3-1.2 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal during shutdown in the event of unavailability of the RHR.
	Residual Heat Removal System (RHR) (see Section 12.3.5.4)	RHR SFC 3-1.2 (12, 13)	The RHR through its Reactor Shutdown Cooling mode is a principal means to deliver long term containment heat removal by removing the decay heat of fission products from the reactor without exceeding the fuel design margins and RCPB design conditions after reactor shutdown following frequent faults such as main condenser unavailability, and infrequent faults such as SBO after power recovery.	

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Long Term Heat Removal- Reactor			SFCs	
Class 1	HLSF 3-1	Residual Heat Removal System (RHR) (see Section 12.3.5.4)	RHR SFC 3-1.3 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as ATWS.
			RHR SFC 3-1.4 (12, 13)	The RHR through its LPFL mode is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as LOCA.
			RHR SFC 3-1.5 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long term containment heat removal upon RHR recovery following venting during infrequent faults such as SBO.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Long Term Heat Removal- Reactor			SFCs	
Class 2	HLSF 3-2	Containment Venting (Atmospheric Control System (AC)) (see Section 13.3.3.4)	AC SFC 3-2.1 (13)	The AC is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.
		Containment Venting (Filtered Containment Venting System (FCVS)) (see Section 13.3.3.4, 16.7.3.5)	FCVS SFC 3-2.1 (13, 16)	The FCVS is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.
Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 1	HLSF 4-2	Safety Relief Valve (SRV) (see Section 12.3.5.2)	NB SFC 4-2.1 (12)	The MS through the safety valve function of the SRVs is the principal means to deliver overpressure protection of the RCPB under abnormal transients and accident conditions that could put excessive pressure on the boundary.
	HLSF 4-7	Primary Containment (see Section 13.3)	PCV SFC 4-7.3 (13)	The air leakage ratio of the RCCV is based on 0.4 percent per day or less of free volume of the containment at ordinary temperature and with a 90 percent of the maximum design pressure.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 1	HLSF 4-7	Flow restrictors (see Section 12.3.5.2)	NB SFC 4-7.1 (12)	The MS through its flow restrictors is a principal means to limit the loss of reactor coolant and the release of radioactive material from the RPV following a MS line rupture outside the PCV to the extent that the RPV water level does not drop below the top of the active fuel before closure of the MSIVs.
		Main Steam Isolation Valve (MSIV) (see Section 12.3.5.2)	NB SFC 4-7.2 (12)	The MS is the principal means to close the MS lines to limit the release of reactor coolant and radioactive material to the surroundings in the event of a MS pipe rupture by closing the MSIVs.
			NB SFC 4-7.3 (12)	The NB components penetrating the primary containment form a barrier to confine radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
		Primary Containment Isolation System (PCIS) (see Section 12.3, 12.4 and 13.3.3.2)	SFC 4-7.1 of each systems (12, 13)	The components penetrating the primary containment form a barrier to confine the radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 2	HLSF 4-7	Secondary Containment (Reactor Building) (see Section 10.4)	R/B SFC 4-7.5 (10)	The R/B provides a sufficiently leak-tight boundary using concrete walls and slabs at that boundary to confine any potential radioactive release inside of the structure. The Standby Gas Treatment System (SGTS) creates a negative air pressure inside the secondary containment during postulated accidental conditions, so that airflow is always from outside to inside. This negative pressure limits a potential radioactive release to the external environment during the fault condition.
		Reactor Area (R/A) Heating Ventilating and Air Conditioning System (HVAC) Isolation Damper (see Section 16.5)	R/A HVAC SFC 4-7.2 (16)	The R/A HVAC system is designed to reduce the release and spread of airborne contamination during basis design and beyond design basis fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 2	HLSF 4-7	Standby Gas Treatment System (SGTS) (see Section 13.3.4.2)	SGTS SFC 4-7.2 (13)	The SGTS constitutes a part of the confinement function in the event of design basis faults such as LOCA, radioactive releases from refuelling operations, etc. by maintaining a negative pressure in the Secondary Containment relative to the outdoor atmosphere, and by filtering radiological effluents from the Primary Containment that leak into the Secondary Containment to control and reduce the release of radioactive substances to the environment.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 2-1	High Pressure Core Flooder System (HPCF) (see Section 13.4)	HPCF SFC 2-1.1 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in high pressure state and in the interval it is being depressurised so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of frequent faults such as loss of the normal feedwater supply and infrequent faults such as LOCA.
			HPCF SFC 2-1.2 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 2-1	Low Pressure Core Flooder System (LPFL) (see Section 13.4)	RHR SFC 2-1.1 (12, 13)	The LPFL is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.
Class 2	HLSF 2-2	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-2.1 (13, 16)	The FLSS is the secondary means to provide reactor core cooling in order to prevent significant damage to the fuel and minimise the reaction between the fuel cladding and the reactor coolant sufficiently so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of design basis faults with all the primary reactor core cooling means (ECCS) have failed.
	HLSF 2-5	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-5.1 (16)	In the eventuality that the cooling function for the SFP is unavailable or small leakage from the SFP occurs, the FLSS supplies sufficient water to maintain the water level of the SFP as a secondary means of cooling the spent fuel stored in the SFP.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 2	HLSF 2-2	Reactor Depressurisation Control Facility (RDCF) (Alternative SRV) (see Section 16.7.3.3)	RDCF SFC 2-2.1 (13, 16)	The RDCF is an alternative means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults where the primary means (ECCS) are not available.
			RDCF SFC 2-2.2 (13, 16)	The RDCF is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS after RCIC operation for the first 24 hours in the event of design basis faults such as SBO or Class 1 CCF.
Class 3	HLSF 2-2	Reactor Depressurisation Control Facility (Switching Valve for SRV) (RDCF) (see Section 16.7.3.3)	RDCF SFC 2-2.3 (13, 16)	The RDCF with switching valves is the principal means to maintain RPV depressurisation in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults such as SBO or Class 1 CCF after the first 24 hours.
		Flooder System of Reactor Building (FLSR) (see Section 16.7.3.2)	FLSR SFC 2-2.2 (16)	The FLSR is a secondary means to provide reactor core cooling during outage in order to prevent significant damage to the fuel in the event of design basis fault where the primary (ECCS) and secondary (FLSS) means for core cooling are failed or unavailable.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 3	HLSF 2-2	Fire Protection System (see Section 16.6.3)	FPS SFC 2-2.1 (16)	The Fire Protection System (FP), which is a system for fire fighting, will be utilised to supply coolant water for reactor core cooling in the event the primary (ECCS) and secondary (FLSS) means for core cooling are failed or unavailable.
Class 1	HLSF 3-1	Safety Relief Valve (SRV) –Manual depressurisation– (see Section 12.3.5.2)	NB SFC 3-1.1 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal to reach reactor cold shutdown by depressurisation of the RPV in the event of unavailability of the main condenser
			NB SFC 3-1.2 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal during shutdown in the event of unavailability of the RHR.
		Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 3-1.1 (12)	The RHR through its Reactor Shutdown Cooling mode is the principal means to remove residual heat after normal reactor shutdown to reach reactor cold shutdown

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 3-1	Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 3-1.2 (12, 13)	The RHR through its Reactor Shutdown Cooling mode is a principal means to deliver long term containment heat removal by removing the decay heat of fission products from the reactor without exceeding the fuel design margins and RCPB design conditions after reactor shutdown following frequent faults such as main condenser unavailability, and infrequent faults such as SBO after power recovery.
			RHR SFC 3-1.3 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as ATWS.
			RHR SFC 3-1.4 (12, 13)	The RHR through its LPFL mode is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 3-1	Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 3-1.5 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long term containment heat removal upon RHR recovery following venting during infrequent faults such as SBO.
Class 2	HLSF 3-2	Containment Venting (Atmospheric Control System (AC)) (see Section 13.3.3.4)	AC SFC 3-2.1 (13)	The AC is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.
		Containment Venting (Filtered Containment Venting System (FCVS)) (see Section 13.3.3.4, 16.7.3.5)	FCVS SFC 3-2.1 (13, 16)	The FCVS is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials – Shutdown modes			SFCs	
Class 1	HLSF 4-7	Primary Containment Isolation System (PCIS) (see Section 12,3, 12.4 and 13.3.3.2)	CUW SFC 4-7.1 (12, 13)	The CUW components penetrating the primary containment form a barrier to confine the radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
		Primary Containment Isolation System (PCIS) (see Section 12,3, 12.4 and 13.3.3.2)	RHR SFC 4-7.1 (12, 13)	The RHR components penetrating the primary containment form a barrier to confine the radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
Others – Shutdown modes			SFCs	
Class 1	HLSF 5-5	Remote Shutdown System (RSS) (see Section 14.6.2.2)	SSLC SFC 5-5.1 (14)	RSS provides the functions to control the systems to shutdown safely from outside the main control room.
	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	FHM SFC 5-6.1 (19)	The FHM, including lifting attachment and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Reactivity Control - SFP			SFCs	
Class 1	HLSF 1-9	Spent Fuel Storage rack (see Sections 19.8.2.2)	SFS SFC 1-9.1 (19)	The spent fuel storage racks maintain the Fuel Assemblies in a subcritical state.
Fuel Cooling - SFP			SFCs	
Class 1	HLSF 2-4	Spent Fuel Storage Pool (SFP) (see Section 19.8)	SFS SFC 2-4.1 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.
		Fuel Pool Cooling and Clean-up System (FPC) (see Section 19.9)	FPC SFC 2-4.1 (19)	The FPC removes heat from the SFP and maintains the SFP water temperature within the designed values by removing decay heat.
		Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 2-4.1 (12, 19)	The RHR provides the FPC with supplemental cooling to maintain the SFP water temperature within the design values by removing decay heat in the event of a full core offload where the heat load to the pool exceeds the FPC cooling capacity. This function can also be used for recovery from potential upper pools cooling failure and subsequent boiling event.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling - SFP			SFCs	
Class 2	HLSF 2-5	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-5.1 (16, 19)	In the eventuality that the cooling function for the SFP is unavailable or small leakage from the SFP occurs, the FLSS supplies sufficient water to maintain the water level of the SFP as a secondary means of cooling the spent fuel stored in the SFP.
Confinement /Containment of Radioactive Materials – SFP			FCs	
Class 1	HLSF 4-7	The check valves and syphon break system (FPC) (see Section 19.9)	FPC SFC 4-7.1 (19)	The check valves and syphon break system prevent potential syphoning from the SFP and subsequent spent fuel exposure in the SFP.
		Spent Fuel Storage Pool (SFP) (see Section 19.8)	SFS SFC 4-7.1 (19)	The SFP, the Cask Pit, and associated SFP gates are designed to prevent loss of SFP water.
			SFS SFC 4-7.2 (19)	The SFP has sufficient water depth to provide radiation protection to operators working on the Operating Deck.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Route Faults			SFCs	
Class 1	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	FHM SFC 5-6.1 (19)	The FHM, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
			FHM SFC 5-6.3 (19)	The FHM handles fuel within the pools system in a subcritical configuration.
Class 1 Class 2	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	FHM SFC 5-6.2 (19)	The FHM, associated lifting attachments and safety systems handle irradiated loads suitably submerged so that radiation shielding is provided.
Class 1	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)	RBC SFC 5-6.1 (19)	The RBC, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
Class 2	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)	RBC SFC 5-6.2 (19)	The RBC, associated lifting attachments and safety systems handle irradiated loads suitably submerged so that radiation shielding is provided.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Route Faults			SFCs	
Class 1	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	NSC SFC 5-6.1 (19)	The Nuclear Special Cranes (NSCs) are designed to prevent a collision between the NSCs or other cranes, resulting from frequent and infrequent faults within the design basis.
Class 1	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)		
Class 2		Fuel Preparation Machine (FPM) (see Section 19.5)		

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Spent Fuel Export			SFCs	
Class 1	HLSF 1-10	Canister basket (see Section 19.10)	SFE SFC 1-10.1 (19)	Fuel remains in a subcritical condition during operations under normal and fault conditions.
Class 1	HLSF 2-4	Spent Fuel Storage Facility (SFS) (see Section 19.8)	SFS SFC 2-4.1 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.
Class 1	HLSF 2-6	Canister (see Section 19.10) Canister Cooling System (CCS) (see Section 19.10) Over Temperature Protection System (OTPS) for Canister Drying (see Section 19.10)	SFE SFC 2-6.1 (19)	Temperature of spent fuel will be maintained within specified limits such that fuel clad does not fail due to overheating during unsealed canister SFE operations and associated fault conditions.
Class 2	HLSF 2-6	Backup Canister Cooling System (BCCS) (see Section 19.10)	SFE SFC 2-6.1 (19)	Temperature of spent fuel will be maintained within specified limits such that fuel clad does not fail due to overheating during unsealed canister SFE operations and associated fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Spent Fuel Export			SFCs	
Class 1	HLSF 2-6	Canister (see Section 19.10)	SFE SFC 2-6.2 (19)	Temperature of spent fuel will be maintained within specified limits such that the fuel clad does not fail due to overheating during sealed canister SFE operations and associated fault conditions.
Class 1	HLSF 4-14	Canister (see Section 19.10)	SFE SFC 4-14.2 (19)	Containment function will be maintained during SFE sealed canister operations and associated fault conditions.
Class 1	HLSF 4-16	Canister (see Section 19.10) Transfer Cask (see Section 19.10)	SFE SFC 4-16.1 (19)	Shielding from spent fuel will reduce dose to operators and public ALARP during normal SFE operations and associated fault conditions.
Class 1 Class 2	HLSF 5-6	Fuel Handling Machine (see Section 19.6) Lifting Attachment (see Section 19.7)	FHM SFC 5-6.1 (19)	The FHM, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
Class 1	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)	RBC SFC 5-6.1 (19)	The RBC, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Spent Fuel Export			SFCs	
Class 1	HLSF 5-16	Canister (see Section 19.10) Transfer Cask (see Section 19.10)	SFE SFC 5-16.1 (19)	Handling of spent fuel within Canister shall not compromise other SFCs and the spent fuel and Casks shall remain retrievable during normal operation and following frequent faults.
Class 2	HLSF 5-16	Cask stand (see Section 19.10)	SFE SFC 5-16.1 (19)	Handling of spent fuel within Canister shall not compromise other SFCs and the spent fuel and Casks shall remain retrievable during normal operation and following frequent faults.
Class 1	HLSF 5-22	Impact Limiters (see Section 19.10)	SFE SFC 5-22.1 (19)	Canister deceleration during design basis drop faults shall remain below allowable limits.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Radioactive Waste Handling and Storage			SFCs	
Class 3	HLSF 4-7	Off Gas System (see Section 18.7)	OG SFC 4-7.1 (18)	The OG minimises the dose to worker during the start-up, power and shutdown operations.
			OG SFC 4-7.2 (18)	The OG mitigates the dose to worker in the event of OG system failure.
Class 3	HLSF 4-7	Tank Vent System (see Section 18.9)	TV SFC 4-7.4 (18)	Doses to public and workers in faults are ALARP and within limits and targets given in PCSR Chapter 5.3: Definition of Design Basis Faults and Beyond Design Basis Faults.
Class 3		HVAC (see Section 16.5)	Rw/B HVAC SFC 4-7.1 (18)	The Rw/B HVAC system is designed to prevent the release and spread of radioactive material during normal operation.
Class 3	HLSF 4-8	Off Gas System (see Section 18.7)	OG SFC 4-8.1 (18)	The OG mitigates the release of gaseous radioactive substances to the environment in the event of OG system failure.
Class 3		Tank Vent System (see Section 18.9)	TV SFC 4-8.1 (18)	The total radioactivity in gaseous discharges to the environment from the Tank Vent Treatment system is minimised.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Radioactive Waste Handling and Storage			SFCs	
Class 3	HLSF 4-11	Off Gas System (see Section 18.7)	OG SFC 4-11.1 (18)	The OG minimises the release of radioactivity to the environment during the start-up, power and shutdown operations.
			OG-SFC-4-11.2 (18)	The OG reduces the risk of hydrogen combustion arising from the reaction of radiolytic hydrogen produced in the reactor.
			OG SFC 4-11.3 (18)	The OG prevents hydrogen combustion in the event of OG Recombiner failure.
Class 3	HLSF 4-12	Liquid Waste Management System (see Section 18.5)	LWMS SFC 4-12.1 (18)	The total radioactivity in liquid discharges to the environment from the LWMS is minimised.
			LWMS SFC 4-12.3 (18)	Doses to both the workers and the public from normal operation of the UK ABWR LWMS are ALARP.
			LWMS SFC 4-12.6 (18)	Doses to public and workers in faults are ALARP and within limits and targets given in PCSR Chapter 5.3: Definition of Design Basis Faults and Beyond Design Basis Faults.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Radioactive Waste Handling and Storage			SFCs	
Class 3	HLSF 5-7	Tank Vent System (see Section 18.9)	TV SFC 5-7.1 (18)	Hydrogen concentrations in vessel ullage spaces will not reach the Lower Flammability Limit (LFL).
Flammability Control			SFCs	
Class 2	HLSF 5-15	Flammability Control System (see Section 13.3.3.3)	FCS SFC 5-15.1	The FCS backs up the confinement function by maintaining the hydrogen and oxygen concentrations in the PCV below the flammability limits through recombination of the gases generated and accumulated in the PCV that might occur after design basis faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-1	Safety System Logic and Control System (SSLC) (see Section 14.6.2.1)	SSLC SFC 5-1.1 (14)	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system as the first provision for the Category A Safety Functions.
			SSLC SFC 5-2.1 (14)	SSLC provides the functions to control the support systems assigned to the first provision for the Category A Safety Functions.
Class 2	HLSF 5-1 HLSF 5-3	Hard Wired Backup System (see Section 14.6.3)	HWBS SFC 5-1.1 (14)	HWBS provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system as the second provision for the Category A Safety Functions.
			HWBS SFC 5-3.1 (14)	HWBS provides the functions to control the support systems for the second provision for the Category A Safety Functions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-2	Class 1 Emergency Power Supply System (EPS) (see Section 15.4.5)	EPS SFC 1 (15) EPS SFC 2 (15) EPS SFC 3 (15) EPS SFC 4 (15) EPS SFC 5 (15)	The EPS supports SSCs providing HLSF associated with FSF 1: Control of Reactivity FSF 2: Fuel Cooling FSF 3: Long Term Heat Removal FSF 4: Confinement and Containment of Radioactive Materials. FSF 5: Others.
		Ultimate Heat Sink (UHS) (see Section 16.3.1)	UHS SFC 5-2.1 (16)	The UHS is the principal means to provide sufficient cooling water to the RSW to dissipate the heat from the plant auxiliaries required for power operation, shutdown operation, hot stand-by with off-site power and main condenser available, hot stand-by under Loss of Off-site Power (LOOP) and main condenser unavailable, and main design basis fault scenarios (LOCA).

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-2	Reactor Building Cooling Water System (RCW) (see Section 16.3.2.1)	RCW SFC 5-2.1 (16)	The RCW is an essential system for supporting HPCF operation by removing heat from the main HPCF components (HPCF Pumps) and transferring it to RSW process water whenever HPCF operation is required.
			RCW SFC 5-2.2 (16)	The RCW is an essential system for supporting EDG operation by removing heat from the EDGs and transferring it to RSW process water whenever EDG operation is required.
			RCW SFC 5-2.3 (16)	The RCW is an essential system for supporting RHR operation by removing heat from the main RHR components (RHR Pumps) and transferring it to RSW process water whenever RHR operation is required.
			RCW SFC 5-2.4 (16)	The RCW is an essential system for supporting Safety Class 1 HVAC operation by removing heat from HVAC components (Safety Class 1 LCUs and HECW Chillers) and transferring it to RSW process water whenever HVAC is operating.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-2	Reactor Building Service Water System (RSW) (see Section 16.3.2.2)	RSW SFC 5-2.1 (16)	The RSW is an essential system for supporting HPCF operation by removing heat from the RCW process water and transferring it to the UHS whenever HPCF operation is required.
			RSW SFC 5-2.2 (16)	The RSW is an essential system for supporting EDG operation by removing heat from the RCW process water and transferring it to the UHS whenever EDG operation is required.
			RSW SFC 5-2.3 (16)	The RSW is an essential system for supporting RHR operation by removing heat from the RCW process water and transferring it to the UHS whenever RHR operation is required.
			RSW SFC 5-2.4 (16)	The RSW is an essential system for supporting Safety Class 1 HVAC operation by removing heat from RCW process water and transferring it to the UHS whenever HVAC is operating.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 2	HLSF 5-3	B/B Class 2 Emergency Power Supply System (EPS) (see Section 15.4.6)	EPS SFC 1 (15) EPS SFC 2 (15) EPS SFC 3 (15) EPS SFC 4 (15) EPS SFC 5 (15)	The EPS supports SSCs providing HLSF associated with FSF 1: Control of Reactivity FSF 2: Fuel Cooling FSF 3: Long Term Heat Removal FSF 4: Confinement and Containment of Radioactive Materials. FSF 5: Others.
		Emergency equipment cooling water system (EECW) (see Section 16.3.6)	EECW SFC 5-3.1 (16)	The EECW is the principal means to remove heat from the Backup Building Generator system (BBG) auxiliaries so that power can be supplied to the BBG loads in the event of frequent design basis faults where BBG loads operation is required.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-18	Heating Ventilating and Air Conditioning System (HVAC) (Class 1) (see Section 16.5)	R/A HVAC SFC 5-18.2 (16) DGEE/Z HVAC SFC 5-18.2 (16) Hx/B HVAC SFC 5-18.2 (16) RBEEE/Z HVAC SFC 5-18.2 (16) CBEEE/Z HVAC SFC 5-18.2 (16) MCR HVAC SFC 5-18.2 (16)	The Class 1 HVACs ensures the adequate environmental parameters are maintained so that the relevant SSCs can function appropriately and can deliver the fundamental safety functions in fault conditions.
		MCR Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5)	MCR HVAC SFC 5-18.5 (16)	The MCR HVAC systems ensure the adequate environmental parameters are maintained for working conditions during fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-18	HVAC Emergency Cooling Water System (HECW) (see Section 16.3.5.1)	HECW SFC 5-18.2 (16)	The HECW provides chilled water for the normal/Emergency and the Emergency HVAC during fault conditions such as LOCA and LOOP.
Class 2	HLSF 5-18	Heating Ventilating and Air Conditioning System (HVAC) (Class 2) (see Section 16.5)	BBECR HVAC SFC 5-18.2 (16) BBEE/Z HVAC SFC 5-18.2 (16) CBC2EE/Z HVAC SFC 5-18.2 (16) FV/B HVAC SFC 5-18.2 (16)	The Class 2 HVACs ensures the adequate environmental parameters are maintained so that the relevant SSCs can function appropriately and can deliver the fundamental safety functions in fault conditions.
		BBECR Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5)	BBECR HVAC SFC 5-18.5 (16)	The BBECR HVAC systems ensure the adequate environmental parameters are maintained for working conditions during fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 2	HLSF 5-18	HVAC Backup Building Cooling Water System (HBCW) (see Section 16.3.5.3)	HBCW SFC 5-18.2 (16)	The HBCW provides chilled water for the normal/Emergency and the Emergency HVAC that is related to the nuclear supporting functions especially important to safety during fault conditions.

* The number in brackets shows the PCSR chapter where the SFC is claimed. The description of the SFCs can be found in Appendix A of the corresponding chapter.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Reactivity Control - Reactor			SFCs	
Class 2	HLSF 1-5	Recirculation Pump Trip (RPT) (see Section 14.6.3)	RRS SFC 1-5.1 (12)	The RIPs of the RRS are tripped by the RPT by a signal from the Hardwired Backup System (HWBS) as part of the actions to perform alternative shutdown of the reactor in the event of ATWS.
		Feed water Stop (see Section 14.6.3)	NB SFC 1-5.1 (12)	The FDW flow is controlled by the Hardwired Back-up System logic in order to prevent reactivity insertion in the event of ATWS.
Fuel Cooling – Reactor			SFCs	
Class 1	HLSF 2-1	Reactor Core Isolation Cooling System (RCIC) (see Section 13.4.1)	RCIC SFC 2-1.1 (13)	The RCIC is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in high pressure state and in the interval it is being depressurised so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of frequent faults such as loss of the normal feedwater supply and infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 1	HLSF 2-1	Reactor Core Isolation Cooling System (RCIC) (see Section 13.4.1)	RCIC SFC 2-1.2 (13)	The RCIC is capable of providing reactor core cooling during at least 8 hours so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of Loss of Offsite Power Supply (LOOP) and loss of all the AC emergency power sources.
		High Pressure Core Flooder System (HPCF) (see Section 13.4.1)	HPCF SFC 2-1.1 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in high pressure state and in the interval it is being depressurised so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of frequent faults such as loss of the normal feedwater supply and infrequent faults such as LOCA.
			HPCF SFC 2-1.2 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 1	HLSF 2-1	Low Pressure Core Flooder System (LPFL) (see Section 13.4.1)	RHR SFC 2-1.1 (12, 13)	The LPFL is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.
		Safety Relief Valve (SRV) -Safety valve function- (see Section 12.3.3)	NB SFC 2-1.1 (12)	The MS through the safety valve function of the SRV is the principal means to release the steam generated during reactor core cooling by high pressure core cooling systems in the event of faults such as LOCA outside the PCV.
		Automatic Depressurisation System (ADS) (see Section 12.3.3, 13.4.1)	NB SFC 2-1.3 (12, 13)	The NB through the ADS is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA inside the PCV.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 1	HLSF 2-1	Transient Automatic Depressurisation System (Transient ADS) (see Section 12.3.3, 13.4.1)	NB SFC 2-1.4 (12, 13)	The NB through the transient ADS is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA outside the PCV.
Class 2	HLSF 2-2	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-2.1 (13, 16)	The FLSS is the secondary means to provide reactor core cooling in order to prevent significant damage to the fuel and minimise the reaction between the fuel cladding and the reactor coolant sufficiently so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of design basis faults with all the primary reactor core cooling means (ECCS) have failed.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling- Reactor			SFCs	
Class 2	HLSF 2-2	Reactor Depressurisation Control Facility (RDCF) (Alternative SRV) (see Section 16.7.3.3)	RDCF SFC 2-2.1 (13, 16)	The RDCF is an alternative means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults where the primary means (ECCS) are not available.
			RDCF SFC 2-2.2 (13, 16)	The RDCF is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS after RCIC operation for the first 24 hours in the event of design basis faults such as SBO or Class 1 CCF.
Class 3	HLSF 2-2	Reactor Depressurisation Control Facility (Switching Valve for SRV) (RDCF) (see Section 16.7.3.3)	RDCF SFC 2-2.3 (13, 16)	The RDCF with switching valves is the principal means to maintain RPV depressurisation in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults such as SBO or Class 1 CCF after the first 24 hours.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Long Term Heat Removal- Reactor			SFCs	
Class 1	HLSF 3-1	Safety Relief Valve (SRV) –Manual depressurisation– (see Section 12.3.5.2)	NB SFC 3-1.1 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal to reach reactor cold shutdown by depressurisation of the RPV in the event of unavailability of the main condenser.
			NB SFC 3-1.2 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal during shutdown in the event of unavailability of the RHR.
	Residual Heat Removal System (RHR) (see Section 12.3.5.4)	RHR SFC 3-1.2 (12, 13)	The RHR through its Reactor Shutdown Cooling mode is a principal means to deliver long term containment heat removal by removing the decay heat of fission products from the reactor without exceeding the fuel design margins and RCPB design conditions after reactor shutdown following frequent faults such as main condenser unavailability, and infrequent faults such as SBO after power recovery.	

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Long Term Heat Removal- Reactor			SFCs	
Class 1	HLSF 3-1	Residual Heat Removal System (RHR) (see Section 12.3.5.4)	RHR SFC 3-1.3 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as ATWS.
			RHR SFC 3-1.4 (12, 13)	The RHR through its LPFL mode is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as LOCA.
			RHR SFC 3-1.5 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long term containment heat removal upon RHR recovery following venting during infrequent faults such as SBO.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Long Term Heat Removal- Reactor			SFCs	
Class 2	HLSF 3-2	Containment Venting (Atmospheric Control System (AC)) (see Section 13.3.3.4)	AC SFC 3-2.1 (13)	The AC is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.
		Containment Venting (Filtered Containment Venting System (FCVS)) (see Section 13.3.3.4, 16.7.3.5)	FCVS SFC 3-2.1 (13, 16)	The FCVS is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.
Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 1	HLSF 4-2	Safety Relief Valve (SRV) (see Section 12.3.5.2)	NB SFC 4-2.1 (12)	The MS through the safety valve function of the SRVs is the principal means to deliver overpressure protection of the RCPB under abnormal transients and accident conditions that could put excessive pressure on the boundary.
	HLSF 4-7	Primary Containment (see Section 13.3)	PCV SFC 4-7.3 (13)	The air leakage ratio of the RCCV is based on 0.4 percent per day or less of free volume of the containment at ordinary temperature and with a 90 percent of the maximum design pressure.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 1	HLSF 4-7	Flow restrictors (see Section 12.3.5.2)	NB SFC 4-7.1 (12)	The MS through its flow restrictors is a principal means to limit the loss of reactor coolant and the release of radioactive material from the RPV following a MS line rupture outside the PCV to the extent that the RPV water level does not drop below the top of the active fuel before closure of the MSIVs.
		Main Steam Isolation Valve (MSIV) (see Section 12.3.5.2)	NB SFC 4-7.2 (12)	The MS is the principal means to close the MS lines to limit the release of reactor coolant and radioactive material to the surroundings in the event of a MS pipe rupture by closing the MSIVs.
			NB SFC 4-7.3 (12)	The NB components penetrating the primary containment form a barrier to confine radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
		Safety Relief Valve (SRV) discharge line within the W/W and quencher (see Section 12.3.5.2)	NB SFC 4-7.4 (12)	The MS through the SRV discharge line quenchers is a principal means to suppress the dynamic loads generated in the PCV when steam discharged via the SRVs condenses in the suppression pool.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials - Reactor			SFCs	
Class 1	HLSF 4-7	Primary Containment Isolation System (PCIS) (see Section 12.3, 12.4 and 13.3.3.2)	SFC 4-7.1 of each systems (12, 13)	The components penetrating the primary containment form a barrier to confine the radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
		Reactor Area (R/A) Heating Ventilating and Air Conditioning System (HVAC) Isolation Damper (see Section 16.5)	R/A HVAC SFC 4-7.2 (16)	The R/A HVAC system is designed to reduce the release and spread of airborne contamination during basis design and beyond design basis fault conditions.
Class 2	HLSF 4-7	Standby Gas Treatment System (SGTS) (see Section 13.3.4.2)	SGTS SFC 4-7.2 (13)	The SGTS constitutes a part of the confinement function in the event of design basis faults such as LOCA, radioactive releases from refuelling operations, etc. by maintaining a negative pressure in the Secondary Containment relative to the outdoor atmosphere, and by filtering radiological effluents from the Primary Containment that leak into the Secondary Containment to control and reduce the release of radioactive substances to the environment.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 2-1	High Pressure Core Flooder System (HPCF) (see Section 13.4)	HPCF SFC 2-1.1 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in high pressure state and in the interval it is being depressurised so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of frequent faults such as loss of the normal feedwater supply and infrequent faults such as LOCA.
			HPCF SFC 2-1.2 (13)	The HPCF is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 2-1	Low Pressure Core Flooder System (LPFL) (see Section 13.4)	RHR SFC 2-1.1 (12, 13)	The LPFL is a principal means to provide reactor core cooling as part of the ECCS when the RPV is in low pressure state so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of infrequent faults such as LOCA.
		Automatic Depressurisation System (ADS) (see Section 12.3.3, 13.4.1)	NB SFC 2-1.3 (12, 13)	The NB through the ADS is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA inside the PCV. In shutdown modes, the Transient ADS is used during the period that the RPV head is in the closed state.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 2-1	Transient Automatic Depressurisation System (Transient ADS) (see Section 12.3.3, 13.4.1)	NB SFC 2-1.4 (12, 13)	The NB through the transient ADS is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA outside the PCV. In shutdown modes, the Transient ADS is used during the period that the RPV head is in the closed state.
Class 2	HLSF 2-2	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-2.1 (13, 16)	The FLSS is the secondary means to provide reactor core cooling in order to prevent significant damage to the fuel and minimise the reaction between the fuel cladding and the reactor coolant sufficiently so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is minimised in the event of design basis faults with all the primary reactor core cooling means (ECCS) have failed.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 2	HLSF 2-2	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-5.1 (16)	In the eventuality that the cooling function for the SFP is unavailable or small leakage from the SFP occurs, the FLSS supplies sufficient water to maintain the water level of the SFP as a secondary means of cooling the spent fuel stored in the SFP.
		Reactor Depressurisation Control Facility (RDCF) (Alternative SRV) (see Section 16.7.3.3)	RDCF SFC 2-2.1 (13, 16)	The RDCF is an alternative means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults where the primary means (ECCS) are not available.
			RDCF SFC 2-2.2 (13, 16)	The RDCF is the principal means to depressurise the RPV in order to provide reactor core cooling in low pressure state with the FLSS after RCIC operation for the first 24 hours in the event of design basis faults such as SBO or Class 1 CCF.
Class 3	HLSF 2-2	Reactor Depressurisation Control Facility (Switching Valve for SRV) (RDCF) (see Section 16.7.3.3)	RDCF SFC 2-2.3 (13, 16)	The RDCF with switching valves is the principal means to maintain RPV depressurisation in order to provide reactor core cooling in low pressure state with the FLSS in the event of design basis faults such as SBO or Class 1 CCF after the first 24 hours.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 3	HLSF 2-2	Flooder System of Reactor Building (FLSR) (see Section 16.7.3.2)	FLSR SFC 2-2.2 (16)	The FLSR is a secondary means to provide reactor core cooling during outage in order to prevent significant damage to the fuel in the event of design basis fault where the primary (ECCS) and secondary (FLSS) means for core cooling are failed or unavailable.
		Fire Protection System (see Section 16.6.3)	FPS SFC 2-2.1 (16)	The Fire Protection System (FP), which is a system for fire fighting, will be utilised to supply coolant water for reactor core cooling in the event the primary (ECCS) and secondary (FLSS) means for core cooling are failed or unavailable.
Class 1	HLSF 3-1	Safety Relief Valve (SRV) –Manual depressurisation– (see Section 12.3.5.2)	NB SFC 3-1.1 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal to reach reactor cold shutdown by depressurisation of the RPV in the event of unavailability of the main condenser
			NB SFC 3-1.2 (12)	The MS through the SRVs is the principal means to deliver long-term residual heat removal during shutdown in the event of unavailability of the RHR.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 3-1	Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 3-1.2 (12, 13)	The RHR through its Reactor Shutdown Cooling mode is a principal means to deliver long term containment heat removal by removing the decay heat of fission products from the reactor without exceeding the fuel design margins and RCPB design conditions after reactor shutdown following frequent faults such as main condenser unavailability, and infrequent faults such as SBO after power recovery.
			RHR SFC 3-1.3 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as ATWS.
			RHR SFC 3-1.4 (12, 13)	The RHR through its LPFL mode is a principal means to deliver long-term containment heat removal following frequent faults such as main condenser unavailability and infrequent faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Cooling and Long Term Heat Removal - Shutdown modes			SFCs	
Class 1	HLSF 3-1	Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 3-1.5 (12, 13)	The RHR through its Suppression Pool Cooling mode (SPC) is a principal means to deliver long term containment heat removal upon RHR recovery following venting during infrequent faults such as SBO.
Class 2	HLSF 3-2	Containment Venting (Atmospheric Control System (AC)) (see Section 13.3.3.4)	AC SFC 3-2.1 (13)	The AC is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.
		Containment Venting (Filtered Containment Venting System (FCVS)) (see Section 13.3.3.4, 16.7.3.5)	FCVS SFC 3-2.1 (13, 16)	The FCVS is a secondary means to deliver long term PCV heat removal and overpressure protection in the event of design basis faults where the primary long-term containment heat removal means (RHR) has failed.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials – Shutdown modes			SFCs	
Class 1	HLSF 4-7	Primary Containment Isolation System (PCIS) (see Section 12,3, 12.4 and 13.3.3.2)	CUW SFC 4-7.1 (12, 13)	The CUW components penetrating the primary containment form a barrier to confine the radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
		Primary Containment Isolation System (PCIS) (see Section 12,3, 12.4 and 13.3.3.2)	RHR SFC 4-7.1 (12, 13)	The RHR components penetrating the primary containment form a barrier to confine the radioactive material within the containment boundary and prevent its dispersion to the environment in the event of faults.
Others – Shutdown modes			SFCs	
Class 1	HLSF 5-5	Remote Shutdown System (RSS) (see Section 14.6.2.2)	SSLC SFC 5-5.1 (14)	RSS provides the functions to control the systems to shutdown safely from outside the main control room.
	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	FHM SFC 5-6.1 (19)	The FHM, including lifting attachment and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Reactivity Control - SFP			SFCs	
Class 1	HLSF 1-9	Spent Fuel Storage rack (see Sections 19.8.2.2)	SFS SFC 1-9.1 (19)	The spent fuel storage racks maintain the Fuel Assemblies in a subcritical state.
Fuel Cooling - SFP			SFCs	
Class 1	HLSF 2-4	Spent Fuel Storage Facility (SFS) (see Section 19.8)	SFS SFC 2-4.1 (19)	The SFS keeps the Fuel Assemblies submerged in water, and provides cooling to the Fuel Assemblies.
		Residual Heat Removal System (see Section 12.3.5.4)	RHR SFC 2-4.1 (12, 19)	The RHR provides the FPC with supplemental cooling to maintain the SFP water temperature within the design values by removing decay heat in the event of a full core offload where the heat load to the pool exceeds the FPC cooling capacity. This function can also be used for recovery from potential upper pools cooling failure and subsequent boiling event.
Class 2	HLSF 2-5	Flooder System of Specific Safety Facility (FLSS) (see Section 16.7.3.1)	FLSS SFC 2-5.1 (16, 19)	In the eventuality that the cooling function for the SFP is unavailable or small leakage from the SFP occurs, the FLSS supplies sufficient water to maintain the water level of the SFP as a secondary means of cooling the spent fuel stored in the SFP.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Confinement /Containment of Radioactive Materials – SFP			SFCs	
Class 1	HLSF 4-7	The check valves and syphon break system (FPC) (see Section 19.9)	FPC SFC 4-7.1 (19)	The check valves and syphon break system prevent potential syphoning from the SFP and subsequent spent fuel exposure in the SFP.
		Spent Fuel Storage Facility (SFS) (see Section 19.8)	SFS SFC 4-7.1 (19)	The SFP, the Cask Pit, and associated SFP gates are designed to prevent loss of SFP water.
		Spent Fuel Storage Pool (SFP) (see Section 19.8)	SFS SFC 4-7.2 (19)	The SFP has sufficient water depth to provide radiation protection to operators working on the Operating Deck.
Fuel Route Faults			SFCs	
Class 1	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	FHM SFC 5-6.1 (19)	The FHM, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
			FHM SFC 5-6.3 (19)	The FHM handles fuel within the pools system in a subcritical configuration.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Route Faults			SFCs	
Class 1 Class 2	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	FHM SFC 5-6.2 (19)	The FHM, associated lifting attachments and safety systems handle irradiated loads suitably submerged so that radiation shielding is provided.
Class 1	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)	RBC SFC 5-6.1 (19)	The RBC, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
Class 2	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)	RBC SFC 5-6.2 (19)	The RBC, associated lifting attachments and safety systems handle irradiated loads suitably submerged so that radiation shielding is provided.
Class 1	HLSF 5-6	Fuel Preparation Machine (FPM) (see Section 19.5)	FPM SFC 5-6.1 (19)	The FPM ensures fuel integrity in the event of a dropped load during normal conditions and frequent and infrequent faults within the design basis.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Fuel Route Faults			SFCs	
Class 1 Class 2	HLSF 5-6	Fuel Preparation Machine (FPM) (see Section 19.5)	FPM SFC 5-6.2 (19)	The FPM handles irradiated loads suitably submerged so that adequate radiation shielding is provided.
Class 1	HLSF 5-6	Fuel Handling Machine (see Section 19.6)	NSC SFC 5-6.1 (19)	The Nuclear Special Cranes (NSCs) are designed to prevent a collision between the NSCs or other cranes, resulting from frequent and infrequent faults within the design basis.
Class 1 Class 2	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7) Fuel Preparation Machine (FPM) (see Section 19.5)		

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Spent Fuel Export			SFCs	
Class 1	HLSF 1-10	Canister basket (see Section 19.10)	SFE SFC 1-10.1 (19)	Fuel remains in a subcritical condition during operations under normal and fault conditions.
Class 1	HLSF 2-6	Canister (see Section 19.10) Canister Cooling System (CCS) (see Section 19.10) Over Temperature Protection System (OTPS) for Canister Drying (see Section 19.10)	SFE SFC 2-6.1 (19)	Temperature of spent fuel will be maintained within specified limits such that fuel clad does not fail due to overheating during unsealed canister SFE operations and associated fault conditions.
Class 2	HLSF 2-6	Backup Canister Cooling System (BCCS) (see Section 19.10)	SFE SFC 2-6.1 (19)	Temperature of spent fuel will be maintained within specified limits such that fuel clad does not fail due to overheating during unsealed canister SFE operations and associated fault conditions.
Class 1	HLSF 2-6	Canister (see Section 19.10)	SFE SFC 2-6.2 (19)	Temperature of spent fuel will be maintained within specified limits such that the fuel clad does not fail due to overheating during sealed canister SFE operations and associated fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Spent Fuel Export			SFCs	
Class 1	HLSF 4-14	Canister (see Section 19.10)	SFE SFC 4-14.2 (19)	Containment function will be maintained during SFE sealed canister operations and associated fault conditions.
Class 1	HLSF 4-16	Canister (see Section 19.10) Transfer Cask (see Section 19.10)	SFE SFC 4-16.1 (19)	Shielding from spent fuel will reduce dose to operators and public ALARP during normal SFE operations and associated fault conditions.
Class 1 Class 2	HLSF 5-6	Fuel Handling Machine (see Section 19.6) Lifting Attachment (see Section 19.7)	FHM SFC 5-6.1 (19)	The FHM, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
Class 1	HLSF 5-6	Reactor Building Overhead Crane (see Section 19.7)	RBC SFC 5-6.1 (19)	The RBC, including lifting attachments and lifted items, handles loads safely such that load path integrity is maintained during normal conditions and frequent and infrequent faults within the design basis.
Class 1	HLSF 5-16	Canister (see Section 19.10) Transfer Cask (see Section 19.10)	SFE SFC 5-16.1 (19)	Handling of spent fuel within Canister shall not compromise other SFCs and the spent fuel and Casks shall remain retrievable during normal operation and following frequent faults.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Spent Fuel Export			SFCs	
Class 2	HLSF 5-16	Cask stand (see Section 19.10)	SFE SFC 5-16.1 (19)	Handling of spent fuel within Canister shall not compromise other SFCs and the spent fuel and Casks shall remain retrievable during normal operation and following frequent faults.
Class 1	HLSF 5-22	Impact Limiters (see Section 19.10)	SFE SFC 5-22.1 (19)	Canister deceleration during design basis drop faults shall remain below allowable limits.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Radioactive Waste Handling and Storage			SFCs	
Class 3	HLSF 4-7	Off Gas System (see Section 18.7)	OG SFC 4-7.1 (18)	The OG minimises the dose to worker during the start-up, power and shutdown operations.
			OG SFC 4-7.2 (18)	The OG mitigates the dose to worker in the event of OG system failure.
Class 3	HLSF 4-7	Tank Vent System (see Section 18.9)	TV SFC 4-7.4 (18)	Doses to public and workers in faults are ALARP and within limits and targets given in PCSR Chapter 5.3: Definition of Design Basis Faults and Beyond Design Basis Faults.
Class 3		HVAC (see Section 16.5)	Rw/B HVAC SFC 4-7.1 (18)	The Rw/B HVAC system is designed to prevent the release and spread of radioactive material during normal operation.
Class 3	HLSF 4-8	Off Gas System (see Section 18.7)	OG SFC 4-8.1 (18)	The OG mitigates the release of gaseous radioactive substances to the environment in the event of OG system failure.
Class 3		Tank Vent System (see Section 18.9)	TV SFC 4-8.1 (18)	The total radioactivity in gaseous discharges to the environment from the Tank Vent Treatment system is minimised.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Radioactive Waste Handling and Storage			SFCs	
Class 3	HLSF 4-11	Off Gas System (see Section 18.7)	OG SFC 4-11.1 (18)	The OG minimises the release of radioactivity to the environment during the start-up, power and shutdown operations.
			OG-SFC-4-11.2 (18)	The OG reduces the risk of hydrogen combustion arising from the reaction of radiolytic hydrogen produced in the reactor.
			OG SFC 4-11.3 (18)	The OG prevents hydrogen combustion in the event of OG Recombiner failure.
Class 3	HLSF 4-12	Liquid Waste Management System (see Section 18.5)	LWMS SFC 4-12.1 (18)	The total radioactivity in liquid discharges to the environment from the LWMS is minimised.
			LWMS SFC 4-12.3 (18)	Doses to both the workers and the public from normal operation of the UK ABWR LWMS are ALARP.
			LWMS SFC 4-12.6 (18)	Doses to public and workers in faults are ALARP and within limits and targets given in PCSR Chapter 5.3: Definition of Design Basis Faults and Beyond Design Basis Faults.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Radioactive Waste Handling and Storage			SFCs	
Class 3	HLSF 5-7	Tank Vent System (see Section 18.9)	TV SFC 5-7.1 (18)	Hydrogen concentrations in vessel ullage spaces will not reach the Lower Flammability Limit (LFL).
Flammability Control			SFCs	
Class 2	HLSF 5-15	Flammability Control System (see Section 13.3.3.3)	FCS SFC 5-15.1	The FCS backs up the confinement function by maintaining the hydrogen and oxygen concentrations in the PCV below the flammability limits through recombination of the gases generated and accumulated in the PCV that might occur after design basis faults such as LOCA.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-1	Safety System Logic and Control System (SSLC) (see Section 14.6.2.1)	SSLC SFC 5-1.1 (14)	SSLC provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system as the first provision for the Category A Safety Functions.
	HLSF 5-2		SSLC SFC 5-2.1 (14)	SSLC provides the functions to control the support systems assigned to the first provision for the Category A Safety Functions.
Class 2	HLSF 5-1	Hard Wired Backup System (see Section 14.6.3)	HWBS SFC 5-1.1 (14)	HWBS provides the functions to generate actuation signals for the engineered safety features and reactor shutdown system as the second provision for the Category A Safety Functions.
	HLSF 5-3		HWBS SFC 5-3.1 (14)	HWBS provides the functions to control the support systems for the second provision for the Category A Safety Functions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-2	Class 1 Emergency Power Supply System (EPS) (see Section 15.4.5)	EPS SFC 1-3 (15) EPS SFC 2-1 (15) EPS SFC 2-4 (15) EPS SFC 2-6 (15) EPS SFC 3-1 (15) EPS SFC 4-7 (15) EPS SFC 5-2 (15) EPS SFC 5-18 (15)	The EPS supports SSCs providing HLSF associated with FSF 1: Control of Reactivity FSF 2: Fuel Cooling FSF 3: Long Term Heat Removal FSF 4: Confinement and Containment of Radioactive Materials. FSF 5: Others.
		Ultimate Heat Sink (UHS) (see Section 16.3.1)	UHS SFC 5-2.1 (16)	The UHS is the principal means to provide sufficient cooling water to the RSW to dissipate the heat from the plant auxiliaries required for power operation, shutdown operation, hot stand-by with off-site power and main condenser available, hot stand-by under Loss of Off-site Power (LOOP) and main condenser unavailable, and main design basis fault scenarios (LOCA).

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-2	Reactor Building Cooling Water System (RCW) (see Section 16.3.2.1)	RCW SFC 5-2.1 (16)	The RCW is an essential system for supporting HPCF operation by removing heat from the main HPCF components (HPCF Pumps) and transferring it to RSW process water whenever HPCF operation is required.
			RCW SFC 5-2.2 (16)	The RCW is an essential system for supporting EDG operation by removing heat from the EDGs and transferring it to RSW process water whenever EDG operation is required.
			RCW SFC 5-2.3 (16)	The RCW is an essential system for supporting RHR operation by removing heat from the main RHR components (RHR Pumps) and transferring it to RSW process water whenever RHR operation is required.
			RCW SFC 5-2.4 (16)	The RCW is an essential system for supporting Safety Class 1 HVAC operation by removing heat from HVAC components (Safety Class 1 LCUs and HECW Chillers) and transferring it to RSW process water whenever HVAC is operating.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-2	Reactor Building Service Water System (RSW) (see Section 16.3.2.2)	RSW SFC 5-2.1 (16)	The RSW is an essential system for supporting HPCF operation by removing heat from the RCW process water and transferring it to the UHS whenever HPCF operation is required.
			RSW SFC 5-2.2 (16)	The RSW is an essential system for supporting EDG operation by removing heat from the RCW process water and transferring it to the UHS whenever EDG operation is required.
			RSW SFC 5-2.3 (16)	The RSW is an essential system for supporting RHR operation by removing heat from the RCW process water and transferring it to the UHS whenever RHR operation is required.
			RSW SFC 5-2.4 (16)	The RSW is an essential system for supporting Safety Class 1 HVAC operation by removing heat from RCW process water and transferring it to the UHS whenever HVAC is operating.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 2	HLSF 5-3	B/B Class 2 Emergency Power Supply System (EPS) (see Section 15.4.6)	EPS SFC 1-5 (15) EPS SFC 2-2 (15) EPS SFC 2-5 (15) EPS SFC 2-6 (15) EPS SFC 3-2 (15) EPS SFC 5-3 (15) EPS SFC 5-18 (15)	The EPS supports SSCs providing HLSF associated with FSF 1: Control of Reactivity FSF 2: Fuel Cooling FSF 3: Long Term Heat Removal FSF 5: Others.
		Emergency equipment cooling water system (EECW) (see Section 16.3.6)	EECW SFC 5-3.1 (16)	The EECW is the principal means to remove heat from the Backup Building Generator system (BBG) auxiliaries so that power can be supplied to the BBG loads in the event of frequent design basis faults where BBG loads operation is required.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-18	Heating Ventilating and Air Conditioning System (HVAC) (Class 1) (see Section 16.5)	R/A HVAC SFC 5-18.2 (16) DGEE/Z HVAC SFC 5-18.2 (16) Hx/B HVAC SFC 5-18.2 (16) RBEEE/Z HVAC SFC 5-18.2 (16) CBEEE/Z HVAC SFC 5-18.2 (16) MCR HVAC SFC 5-18.2 (16)	The Class 1 HVACs ensures the adequate environmental parameters are maintained so that the relevant SSCs can function appropriately and can deliver the fundamental safety functions in fault conditions.
		MCR Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5)	MCR HVAC SFC 5-18.5 (16)	The MCR HVAC systems ensure the adequate environmental parameters are maintained for working conditions during fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 1	HLSF 5-18	HVAC Emergency Cooling Water System (HECW) (see Section 16.3.5.1)	HECW SFC 5-18.2 (16)	The HECW provides chilled water for the normal/Emergency and the Emergency HVAC during fault conditions such as LOCA and LOOP.
Class 2	HLSF 5-18	Heating Ventilating and Air Conditioning System (HVAC) (Class 2) (see Section 16.5)	BBECR HVAC SFC 5-18.2 (16) BBEE/Z HVAC SFC 5-18.2 (16) CBC2EE/Z HVAC SFC 5-18.2 (16) FV/B HVAC SFC 5-18.2 (16)	The Class 2 HVACs ensures the adequate environmental parameters are maintained so that the relevant SSCs can function appropriately and can deliver the fundamental safety functions in fault conditions.
		BBECR Heating Ventilating and Air Conditioning System (HVAC) (see Section 16.5)	BBECR HVAC SFC 5-18.5 (16)	The BBECR HVAC systems ensure the adequate environmental parameters are maintained for working conditions during fault conditions.

Table A-2 SFCs relating to safety systems claimed in Fault Studies (Continued)

Others – Support Systems			SFCs	
Class 2	HLSF 5-18	HVAC Backup Building Cooling Water System (HBCW) (see Section 16.3.5.3)	HBCW SFC 5-18.2 (16)	The HBCW provides chilled water for the normal/Emergency and the Emergency HVAC that is related to the nuclear supporting functions especially important to safety during fault conditions.

In a number of faults, particularly those during shutdown, some of the above SSCs rely on manual initiation. These Operator actions correspond to Human based Safety Claims (HBSCs) that are described in Chapter 27. These HBSCs are listed below in Table A-3. Details can be found in Chapter 27 Appendix A.

It is noted that HBSCs marked with “*” use a SFC which the HF specialists consider to be corrected but does not necessarily exist yet within the related BSC. These items will be confirmed or altered through the live engineering schedule management process.

Table A-3 Human Based Safety Claims

HLSF	HBSC	
1-3	HF CRD 1-3.1_1	Operator recognises specific plant conditions where shutdown is required and manually SCRAMs the reactor using normal SCRAM hard switches on the MCC.
1-5	HF SLC 1-5.1_01	CRO manually initiates ARI from the HWBP as back-up to both the automated and manual RPS SCRAM (A1) functions, and the automated ARI (A2) function.
	HF CRD 1-5.1_01	CRO manually initiates SLC from the HWBP as back-up to the automated and manual RPS SCRAM (A1) and ARI (A2) functions, and the automated SLC (A2) function.
2-1	HF SSLC 2-3.1.1_01*	CRO manually initiates the automatic alignment and start sequence for HPCF(B) or HPCF(C) from the MCC to replenish reactor water level in support of decay heat removal function (during shutdown faults).
	HF HPCF 2-1.1_02	CRO manually switches the HPCF(C) water source from the Condensate Storage Tank (CST) to the Suppression Pool (S/P) using the SAuxP.
	HF HPCF 2-3.1_01*	CRO manually aligns and initiates HPCF(C) from the SAuxP to replenish reactor water level in support of decay heat removal function (during shutdown faults).
	HF HPCF 2-3.1_02*	CRO manually aligns and initiates HPCF(B) from the Division II RSP to replenish reactor water level in support of decay heat removal function (during shutdown faults).

Table A-3 Human Based Safety Claims (Continued)

HLSF	HBSC	
2-1	HF SSLC 2-3.1.3_01*	CRO manually initiates reactor depressurisation to support replenishment of reactor coolant level in decay heat removal function using the Automatic Depressurisation System (ADS) initiation switches on the MCC.
	HF NB 2-3.1_01*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the SRV hardwired switches on the WDP.
	HF NB 2-3.1_03*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Automatic Depressurisation System (ADS) SRV hardwired switches on the RSP.
	HF SSLC 2-3.1.2_01*	CRO manually initiates the automatic alignment and start sequence of RHR in LPFL mode from the MCC to replenish reactor water level in support of decay heat removal function (during shutdown faults).
2-2	HF RDCF 2-3.1_01*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the HWBP (in DBFs, BDBFs).
	HF RDCF 2-3.1_02*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the BBCP (in DBFs).
	HF FLSS 2-3.1_01*	CRO manually initiates FLSS for RPV injection from the HWBP to replenish reactor coolant level in support of decay heat removal function (DBFs, BDBFs).
	HF FLSS 2-3.1_02*	CRO manually initiates FLSS for RPV injection from the BBCP to replenish reactor coolant level in support of decay heat removal function (DBFs).
	HF FLSR 2-3.1_01*	FO manually aligns and connects the FLSR mobile pump unit to the port for RPV injection outside the R/B as a defence in depth back-up to normal and other back-up fuel cooling systems (DBFs).

Table A-3 Human Based Safety Claims (Continued)

HLSF	HBSC	
2-2	HF RDCF 2-3.1_01*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the HWBP (in DBFs, BDBFs).
	HF RDCF 2-3.1_02*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the BBCP (in DBFs).
	HF FLSS 2-3.1_01*	CRO manually initiates FLSS for RPV injection from the HWBP to replenish reactor coolant level in support of decay heat removal function (DBFs, BDBFs).
	HF FLSS 2-3.1_02*	CRO manually initiates FLSS for RPV injection from the BBCP to replenish reactor coolant level in support of decay heat removal function (DBFs).
	HF FLSR 2-2.2_01*	FO manually aligns and connects the FLSR mobile pump unit to the port for RPV injection outside the R/B as a defence in depth back-up to normal and other back-up fuel cooling systems (DBFs).
2-5	HF FLSS 2-3.2_01*	CRO manually initiates FLSS for SFP spray from the HWBP to replenish reactor coolant level via the SFP in support of decay heat removal function (DBFs).
	HF FLSS 2-5.1_01	CRO manually initiates FLSS for SFP spray from the HWBP to make up SFP water level during SFP design-basis faults.
3-1	HF SSLC 3-1.1.2_01	CRO manually initiates reactor depressurisation to support long-term heat removal using the Automatic Depressurisation System (ADS) initiation switches on the MCC.
	HF NB 3-1.1_01	CRO manually depressurises the reactor to support long-term heat removal using the SRV hardwired switches on the WDP.
	HF NB 3-1.1_03	CRO manually depressurises the reactor to support long-term heat removal using the Automatic Depressurisation System (ADS) SRV hardwired switches on the RSP.

Table A-3 Human Based Safety Claims (Continued)

HLSF	HBSC	
3-1	HF SSLC 3-1.1.1_01	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in shutdown cooling (SDC) mode using the MCC.
	HF SSLC 3-1.1.3_01	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in suppression pool (S/P) cooling mode using the MCC.
	HF RHR 3-1.2_01	CRO manually aligns and initiates RHR(C) in shutdown cooling (SDC) mode using the SAuxP.
	HF RHR 3-1.2_02	CRO manually aligns and initiates RHR(A) or RHR(B) in shutdown cooling (SDC) mode from the RSPs.
	HF RHR 3-1.4_01	CRO manually aligns and initiates RHR(C) in suppression pool (S/P) cooling mode using the SAuxP.
	HF RHR 3-1.4_02	CRO manually aligns and initiates RHR(A) or RHR(B) in suppression pool (S/P) cooling mode using the RSPs.
	HF RCW 3-1.2_01	CRO manually aligns and initiates RCW(C) from the SAuxP (to support RHR long-term and containment heat removal functions).
	HF RCW 3-1.2_02	CRO manually aligns and initiates RCW(A) or RCW(B) from the RSPs (to support RHR long-term and containment heat removal functions).
	HF HPCF 3-2.1_01*	During HPCF injection when the S/P temperature increases to a certain temperature, CRO switches the water source back to Condensate Storage Tank (CST) from the Suppression Pool (S/P) using the SAuxP.
3-2	HF AC 3-2.1_01	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs, using the Atmospheric Control (AC) System controls on the MCC.
	HF AC 3-2.1_02 (with HF FCVS 3-2.1_01)	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs, using switches on the HWBP to align and open the valves of the Atmospheric Control (AC) System.

Table A-3 Human Based Safety Claims (Continued)

HLSF	HBSC	
3-2	HF FCVS 3-2.1_01 (with HF AC 3-2.1_02)	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs, using switches on the HWBP to align and open the valves of the Filtered Containment Vent System (FCVS).
	HF FCVS 3-2.2_01 (with HF AC 3-2.1_03)	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs and BDBFs, using switches on the HWBP to align and open the valves of the Filtered Containment Vent System (FCVS).
	HF FCVS 3-2.2_02	CRO manually initiates containment venting, in DBFs and BDBFs and severe accidents, using switches on the BBCP to align and open the valves of the Filtered Containment Vent System (FCVS) or Atmospheric Control (AC) System.
	HF SSLC 4-7.1.1_01	CRO initiates the automated closure of the containment valves using the Primary Containment Isolation System (PCIS) initiation switch.
4-7	HF CUW 4-7.1_01 (with HF LDS 4-7.1_02)	CRO manually isolates the CUW inlet line using the MCC.
	HF LDS 4-7.1_01 (with HF RHR 4-7.1_01)	CRO manually isolates the RHR inlet line using the MCC.
	HF LDS 4-7.1_02 (with HF CUW 4-7.1_01)	CRO manually isolates the CUW inlet line using the MCC.
	HF LDS 4-7.1_03	CRO manually isolates the drain line using the MCC.
	HF RHR 4-7.1_01 (with HF LDS 4-7.1_01)	CRO manually isolates the RHR inlet line using the MCC.
	HF NB 4-7.2_01	CRO closes the MSIVs to isolate the RPV using the MCC.

Appendix B Table of SPC Claims

The safety systems and their corresponding SFCs listed in Appendix A are claimed in Chapter 24 to demonstrate that the relevant Acceptance Criteria are met. The claims on the safety systems assume that at least one division of multi-divisional safety systems are available. This in turn is effectively an assumption that the claimed safety systems fulfil the generic Safety Property Claims listed in Chapter 5 Table 5.3-1 and linked to specific NSEDPs. For any given safety system, the demonstration that the SPCs are fulfilled can be found in the corresponding Basis of Safety Case referenced in the chapter indicated in Table A-2. Details of how essential support systems support these SPCs can be found in [Ref-34].

The Safety Property Claims assumed in Chapter 24 are shown in Table B-1.

Table B-1 Safety Property Claims assumed for safety systems claimed in Fault Studies

SPC	Guide Word	Claim	Relevant NSEDPs
ABC SPC 1	Defence in Depth	System <i>ABC</i> has sufficient defence in depth to meet all relevant accident conditions, including suitable independence and diversity and suitable resilience to DBA, BDBA and SA events.	BP4.2, BP4.5, SP4.10.2, SP8.11.2, FP12, SP12.2.4
ABC SPC 2	Category and Class	The safety functions allocated to system <i>ABC</i> have been categorised and the SSCs classified in accordance with Hitachi-GE's SCDM	BP4.6, SP4.6.1, SP4.6.2
ABC SPC 3	Reliability	The architecture of system <i>ABC</i> achieves the required reliability.	BP 4.10
ABC SPC 4	Fault Tolerance	System <i>ABC</i> is designed, selected and implemented to be tolerant of faults and tolerant of or resilient against failures caused by all relevant internal and external hazards (detailed in the fault schedule).	BP4.1, BP4.9, SP4.9.1, SP4.10.1, SP12.2.4
ABC SPC 6	Lifecycle	The <i>ABC</i> design and selection considers all stages of the plant and hazard life cycles, including operation (including examination, maintenance, inspection and testing), in-life replacement and decommissioning. This also includes confirmation that components have been suitably	SP4.5.1, SP4.6.3, SP4.10.4, SP5.2.5, BP8.1, BP8.2, BP8.5, BP8.6, BP8.8, BP8.9, BP8.10, SP8.10.1, BP11.3, SP13.2.3, SP15.1.1

Table B-1 Safety Property Claims assumed for safety systems claimed in Fault Studies

SPC	Guide Word	Claim	Relevant NSEDPs
		qualified in accordance with Hitachi-GE qualification process.	
ABC SPC 7	Human factors	Dependence on human actions for nuclear safety has been minimised to ALARP and human actions and human factors good practice have been taken into account in the design, the human interfaces and the operating procedures.	BP4.12, SP4.12.3, SP4.12.6, BP5.4, FP15

Appendix C Document Map

