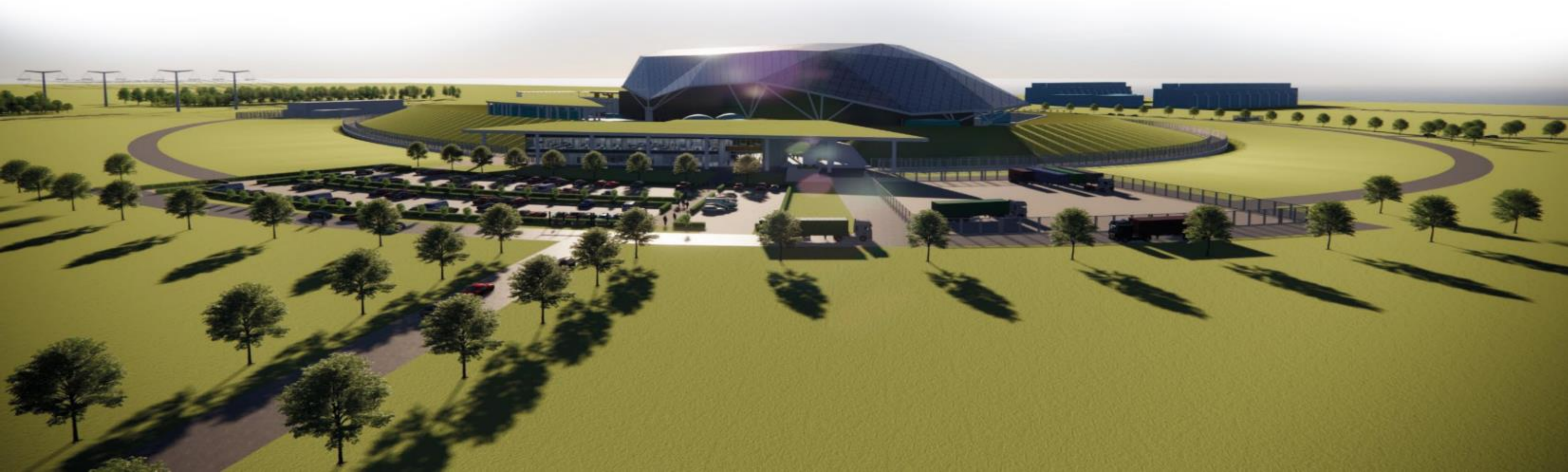
Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 15: Safety Analysis



Record of Change

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First issue of E3S Case
March 2024	2	Issue	This issue incorporates outputs of the safety analysis undertaken up to Reference Design (RD) 7, aligned to Design Reference Point 1, with some of the modelling at RD6 maturity, including: • Deterministic and performance analysis of selected key bounding faults, for design-basis safety measures • Preliminary Severe Accident Analysis (SAA) of selected fault sequences • Preliminary PSA for faults in Modes 1 and 2 • Preliminary internal and external hazard analyses
May 2024	3	Issue	Further updates including: Section 15.2: • Aims of PIE definition methodology discussed • Removal of the term “HAZID studies” • Added PIE categories • Added a description of how DEC-A sequences will be identified and analysed • Confirmed that the fault schedule demonstrates that adequate protection is available for ICFs and LOCAs Section 15.5: • Added an overview of the justification for selection of bounding design basis faults for analysis at the current stage • Information relating to the design of severe accident SSCs has been removed and replaced with references to chapters 6, 7 and 8 Section 15.9: • Conclusions revised to provide a consolidated ALARP statement and forward look Throughout the chapter, editorial updates and clarifications made.

Executive Summary

This chapter of the Environment, Safety, Security and Safeguards (E3S) Case presents the safety analysis of the Rolls-Royce Small Modular Reactor (RR SMR). The chapter outlines the arguments and preliminary evidence available at the design reference point 1 (DRP 1) design stage to underpin the high-level Claim that “the safety analysis has informed the RR SMR design to provide suitable and sufficient levels of defence-in-depth (DiD) to deliver the fundamental safety functions (FSF) and reduce nuclear safety risks to workers and the public to as low as reasonably practicable (ALARP).”

The safety analysis reported includes deterministic, probabilistic, and internal and external hazards analyses. At DRP 1, this includes evidence that provides confidence that the risks associated with the RR SMR can be reduced to ALARP, including:

1. Identification of postulated initiating events (PIEs) for intact circuit/plant faults (ICFs) and loss of cooling accidents (LOCAs) and other fault groups during all operating modes.

2. Development of the fault schedule and fault sequences for each PIE identified, with prevention, protection, and mitigation safety measures against all identified fault sequences to deliver their safety functions demonstrating appropriate levels of DiD. This informs the specification of safety categorised functional requirements in accordance with the E3S categorisation and classification methodology.

3. Preliminary performance analysis of selected key bounding fault sequences to demonstrate that the design-basis safety measures perform as expected. This provides confidence in the design and further work will continue to analyse fault sequences.

4. Preliminary severe accident analysis (SAA) demonstrates that for a limited number of reasonably bounding event sequences assessed, the claimed structures, systems and components (SSCs) (as part of variant four of Containment Safety Measure (CSM) [JM01]) are predicted to successfully prevent or mitigate severe accident phenomena associated with design extension condition-B (DEC-B).

5. Preliminary Level 1 probabilistic safety assessment (PSA) has demonstrated that the early design has a core damage frequency (CDF) that is above the lower RR SMR numerical target for CDF but less than an order of magnitude of it. Further work in this topic will expand the scope and detail of the PSA, refine modelling assumptions, and provide a better understanding of the CDF of the design.

6. The process that is informing the RR SMR design and layout to inherently minimise internal hazards risks are described. Internal hazards for RR SMR have been identified and analysis has been undertaken, the output of the analysis is used to inform the design development. No major shortfalls or issues have been identified against IH requirements.

7. Individual and combined external hazards applicable to the generic design of the RR SMR have been screened with the production of a generic site envelope (GSE) for Great Britain (GB) and a combined external hazards report. Methodologies have also been developed on space weather and accidental aircraft crash, as well as beyond design basis faults, which shall be applied in the development of the design. Additionally, external hazards measures are in development, which includes the Hazard Shield and Base Isolation.

This chapter provides an overview of the arguments and evidence available at the current stage of development to support the E3S claims and sub-claims. Further evidence to support the top-level claim and sub-claims will be presented as the E3S Case is progressed alongside the design programme.

Contents

Tables

Figures

15.0 Introduction

15.0.1 Introduction to Chapter

Chapter 15 of the Rolls-Royce Small Modular Reactor (RR SMR) generic Environment, Safety, Security and Safeguards (E3S) Case presents the overarching summary and entry point to the safety analysis for the RR SMR.

15.0.2 Scope and Maturity

The scope of the safety analysis presented in this chapter covers both deterministic and probabilistic safety assessment, as well as assessment of internal hazards and external hazards. This includes consideration of Design Basis Conditions (DBCs) and design extension conditions (DECs), including DEC-A and DEC-B severe accidents.

The safety analysis covers all aspects of the RR SMR, including Reactor Island, Turbine Island, Cooling Water Island and Balance of Plant. It covers all modes of operation for the RR SMR, as defined in E3S Case Tier 1 Chapter 13: Conduct of Operations [1], and all lifecycle phases, noting there is limited maturity for some operating modes as detailed below.

The process to demonstrate the flow of Operational Limits and Conditions (OLCs) from the safety analysis into operational documentation is outlined in E3S Case Tier 1 Chapter 16: Operational Limits and Conditions [2], and is not covered in this chapter.

Version 2 of the generic E3S Case is based on the reference design 7 (RD7), corresponding to Design Reference Point 1 (DRP 1) for the Generic Design Assessment (GDA). Safety analysis naturally lags the design, therefore while Structures, Systems, and Components (SSCs) are presented at DRP1, the inputs to the safety analysis presented within this issue of the E3S case do not always directly align to DRP1. The status of the safety analysis at RD7/DRP1 that is summarised within this chapter is:

- Deterministic safety analysis (DSA) reflects the DRP1 maturity and covers fault schedule development for all operating modes and DBCs. Reactor faults are covered in detail, whereas faults for other plant areas such as Spent Fuel Pool (SFP), refuelling operations and waste systems are covered in a preliminary way only. The supporting performance analysis for reactor faults covers a subset of key bounding faults and the models are based on pre-DRP1 maturity (RD6).

- SAA reflects design maturity at RD6 and represents a limited number of reasonably bounding DEC-B sequences which are used to establish a basis for the design and performance of severe accident SSCs. SAA at RD6 informs the RD7/DRP1 design. The next iteration of SAA will reflect RD7/DRP1.

- Probabilistic safety assessment (PSA) includes a Level 1 Internal Events at power PSA model encompassing reactor operating modes 1 and 2. Inputs were taken from the RD6 level of design maturity of reactor systems and the Fault Schedule developed from the RD5 level of design maturity.

- Internal hazards analysis for Reactor Island has been carried out based on a design point prior to the DRP1 design (at RD6) due to the design maturity available at the time of analysis. The scope of the internal hazards analysis has largely concentrated on Reactor Island because this is the location of nuclear safety systems. Analysis has also taken place for systems and buildings outside of the hazard shield at a higher level than the analysis in Reactor Island, due to the level of design maturity available. The internal hazards analysis outside of the hazard shield is based on the DRP1 design.

- External hazards applicable to the generic design of the RR SMR have been screened with initial development of a generic site envelope (GSE) for Great Britain (GB).

The conclusions of this chapter provide a forward look of information still to be developed for chapter 15 to achieve the generic E3S Case objective.

15.0.3 Claims, Arguments and Evidence Route Map

The overall approach to Claims, Arguments, Evidence (CAE) and set of fundamental E3S claims to achieve the E3S fundamental objective are described in E3S Case Tier 1 Chapter 1: Introduction [3]. The associated top-level chapter claim for E3S Case Tier 1 Chapter 15: Safety Analysis is:

Claim 15: Safety analysis informs the design and demonstrates there is suitable and sufficient defence in depth to deliver the fundamental safety functions, and that nuclear safety risks to workers and the public are reduced to ALARP.

A decomposition of this claim into sub-claims, and mapping to the relevant Tier 2 and Tier 3 information containing the detailed arguments and evidence, is presented in the E3S Case Route Map [4]. Given the evolving nature of the E3S Case alongside the maturing design, the underpinning arguments and evidence may still be developed in future design stages; the trajectory of this information, where possible, is also illustrated in the route map.

A proportionate summary of the arguments and evidence from lower tier information, available at the current design stage, is presented within this chapter. A mapping of the claims to the corresponding sections that summarise the arguments and/or evidence is provided in Appendix A (section 15.11).

15.0.4 Applicable Regulations, Codes and Standards

The RR SMR interpretation of regulations, codes and standards applicable across all areas of E3S are presented in the E3S Design Principles [5].

Additional codes and standards have been used to inform Rolls-Royce SMR technical requirements for safety analysis and include:

- Published regulatory guidance (e.g., Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs))
- International Atomic Energy Agency (IAEA) General Safety Guides
- International Organization for Standardization (ISO)
- European Committee for Standardization (CEN)
- Western European Nuclear Regulators' Association (WENRA) guidance on new Nuclear Powerplant Design and Safety Reference Levels for Existing Reactors

- European Utility Requirements (EUR).

Additional codes and standards relevant to DSA include:

- Nuclear Regulatory Commission (NRC) Policy Issue, SECY-93-087
- IAEA Deterministic Safety Analysis for Nuclear Power Plants [6]
- Section 15.5.1 discusses codes and standards used in the development of the performance analysis methodology.

Additional codes and standards relevant to SAA include:

- IAEA Deterministic Safety Analysis for Nuclear Power Plants [6]
- Reactor Harmonisation Working Group, Practical Elimination Applied to New Nuclear Power Plant (NPP) Designs - Key Elements and Expectations [7].

Additional codes and standards relevant to PSA include:

- IAEA PSA Specific Safety Guides
- IAEA-TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants .

Additional codes and standards relevant to hazards include:

- IAEA Hazard Specific Safety Guides [8] [9]
- IAEA-TECDOC-1944, Fire Protection in Nuclear Power Plants [10]
- Eurocodes
- United States (US) NRC Regulatory Guides
- US NRC NUREGs publications.

15.1 General Considerations

15.1.1 Introduction

The following sections describe the general approaches adopted for each plant state, from normal operation through to design extension conditions with core melt, and internal and external hazards.

15.1.2 Scope of Safety Analysis and Approach Adopted

The overall scope of the safety analysis is described in section 15.0.2. The analysis will be conducted to cover all areas of the plant, all modes of operation and all fault types. The scope of the analysis carried out to-date is presented in this section.

15.1.3 Analysis of Design Basis Conditions

DBCs refer to a set of postulated events which, if unmitigated, could lead to radiological doses to workers and/or a member of the public above certain threshold levels. Such conditions are derived based on fault and hazard identification; these include techniques such as Hazard and Operability (HAZOP) studies, Structured-What-If-Techniques (SWIFTs), Failure Mode and Effects Analysis (FMEAs), and reviews of Relevant Good Practice (RGP) and Operational Experience (OPEX). The identified faults are grouped and bounded into a set of Postulated Initiating Events (PIEs), which are then categorised into fault types such as Intact-Circuit Faults (ICFs) and Loss-of-Coolant Accidents (LOCAs).

Provisions for the prevention, protection and mitigation against DBC events are incorporated into the design, enhancing the safety of the nuclear power plant; these provisions are also called the claimed Safety Measures. The combinations of PIEs together with relevant Safety Measures form sequences, which are categorised into DBC-1 to DBC-4 plant states according to the definitions in E3S Chapter 3 [11]; each plant state is associated with success criteria as defined in E3S Chapter 3 [11]. For instance:

- For frequent faults with first line of protection Safety Measures (DBC-2ii or DBC-3i) the success criterion is no fuel failure.

- For frequent faults with second line of protection Safety Measures (DBC-4) the success criterion is maintaining coolable core geometry with containment remaining intact, and radioactive material confined by at least one physical barrier.

- For infrequent faults (DBC-3ii or DBC-4 depending on the Initiating Event Frequency (IEF)) the success criterion is maintaining coolable core geometry with containment remaining intact, and radioactive material confined by at least one physical barrier.

The safety measures on the RR SMR are capable of achieving a safe and stable state without the need for interim measures to deliver an interim controlled state.

The key Safety Measures that are claimed as protection against DBCs are Scram, Alternative Shutdown Function (ASF), Passive Decay Heat Removal (PDHR), Emergency Core Cooling (ECC) and Containment; these are described in E3S Chapter 6 [12]. Other measures are identified for SFP, fuel and mechanical handling, waste system faults and non-fuel melt faults.

Plant performance analysis is subsequently used to demonstrate that the claimed Safety Measures deliver the relevant plant state success criteria. At DRP1, analysis for the following set of key PIEs has been carried out:

- Loss of pumped primary flow
- Large and intermediate break LOCA
- Main Steam Line Break (MSLB)
- Loss Of Offsite Power (LOOP), including Station BlackOut (SBO)
- Turbine trip
- Steam Generator Tube Rupture (SGTR).

An overview of the justification for selection of these bounding faults is provided in Section 15.5.3.

This repertoire of fault analysis will be broadened from this set of key PIEs to cover the full suite of PIEs as the design matures and will be presented in future versions of this E3S chapter.

The performance analysis also influences the design by informing choices of Control and Instrumentation (C&I) trip parameters and setpoints and informing performance parameters such as pump capacities and tank volumes.

The safety measures are designed in line with the deterministic design criteria that are set out in the E3S design principles in E3S Chapter 3 [11]. This includes criteria such as redundancy, diversity, separation and segregation. The safety functions that characterise the safety measures are assigned safety categories according to the methodology set out in E3S Chapter 3 [11].

Analysis of radiological consequences is carried out as discussed in 15.5.8.

In addition to the deterministic analysis, probabilistic analysis of DBCs is also carried out, in the form of a Level 1 PSA. This brings together the Initiating Event Frequencies (IEFs) with the failure frequencies of the claimed safety measures and calculates an overall Core Damage Frequency (CDF) and allows other numerical insights to inform the design.

15.1.4 Analysis of Design Extension Conditions

DECs refer to a set of postulated accidents which are more severe than those addressed in the design basis or involving additional failures. Such conditions are derived based on deterministic analyses, probabilistic analyses and engineering judgement. Provisions for the mitigation against DEC accidents are incorporated into the design, enhancing the safety of the nuclear power plant. Analysis is subsequently used to demonstrate that the plant can withstand DEC-A and DEC-B conditions where reasonably practicable and that the associated risks are ALARP. The plant is expected to withstand DECs without unacceptable radiological consequences.

DECs are split into two categories, termed DEC-A and DEC-B. The first of these categories (DEC-A) refers to DECs which do not result in significant fuel degradation. DEC-B describes scenarios where core melt occurs.

DEC-A measures are incorporated into the design to prevent significant fuel degradation during complex accident sequences; the success criteria for DEC-A are in line with design basis success criteria for DBC-4.

DEC-B measures prevent or mitigate severe accident phenomena during a postulated core-melt. The RR SMR is designed so that it can be brought into a controlled state (a severe accident safe state[1]) and the containment function can be maintained. Deterministic DEC-B safety analysis (SAA of DEC-B) aims to demonstrate that the safety criteria are met with a high confidence level for potential scenarios involving fuel melt and that where reasonably practicable a severe accident safe state can be reached, with the result that the possibility of plant states arising that could lead to an early radioactive release, or a large radioactive release is 'practically eliminated'.

Releases which are deemed to be 'large' or 'early' will be demonstrated to be 'practically eliminated' such that severe accident phenomena are either physically impossible or determined to be extremely unlikely to occur with a high degree of confidence. Where individual phenomena or event/fault sequences are identified that challenge practical elimination targets, design enhancements will be evaluated to meet these targets where reasonably practicable. The overall objective is to ensure risks are ALARP.

The envisaged approach for the demonstration of practical elimination of relevant accident sequences is discussed within Section 15.5.5.9, where not deemed impossible by design, severe accident event sequences/phenomena will be demonstrated to be managed/mitigated through the provision of design features (incorporated in Defence-in-Depth (DiD) levels 1-4) making large or early release practically eliminated due to being extremely unlikely to occur with a high degree of confidence. Both probabilistic (based on frequency targets) and deterministic (based on design provision) arguments will be provided for event sequences/phenomena deemed to be practically eliminated. High level deterministic practical elimination arguments are provided within Section 15.5.5.9, these will be updated with probabilistic arguments provided following DRP3.

The aim of the E3S Case is to provide the evidence to underpin the claims and arguments, as stated within Section 15.11, which signposts to relevant sections within this chapter which substantiate claims. Such claims sit under the top-level claim; "safety analysis informs the design and demonstrates there is suitable and sufficient DiD to deliver the Fundamental Safety Functions (FSFs), and that nuclear safety risks to workers and the public are reduced to ALARP" as discussed in Section 15.0.3.

The heading structure of the SAA section of this chapter is outlined in 15.5.5.

The development of the plant model used for SAA is discussed within Section 15.5.5.6. An overview of the severe accident management strategy is provided in Section 15.5.5. Following this is a description of potential severe accident phenomena and progression related to the RR SMR and the identification of severe accident mitigative measures based on an understanding of severe accident phenomena and progression related to the RR SMR, and how analysis informs the design of such measures.

A brief description of severe accident mitigative measures, including functional requirements, success criteria, categorisation and classification and supporting system/area interfaces is provided

[1] In the case of DEC-B, the plant achieves a severe accident safe state if the following conditions are met; fuel debris has solidified, and temperature is stable or decreasing; fuel debris heat is being removed and transferred to a heat sink; debris configuration is such that K_{eff} is well below 1; the containment pressure is so low that, in case of a containment opening, the releases of radioactive material are kept within acceptable limits and the evolution of fission products from the fuel debris is ceased [5].

in Section 15.5.5.5. A summary of the results of SAA for DEC-B is then presented within Section 15.5.5.6.1 to Section 15.5.5.6.4, describing how acceptance criteria are met for scenarios analysed to ensure that in the event of a postulated severe accident, that a severe accident safe state is maintained.

Practical elimination arguments for phenomena and sequences which could potentially lead to an early radioactive release or a large radioactive release within the RR SMR are discussed within Section 15.5.5.9 Such phenomena/sequences postulated to result in a large or early release include:

- Rupture of a large pressure-retaining component in the Reactor Coolant System (RCS)
- Fast reactivity insertion accidents
- Direct Containment Heating (DCH)
- Large steam explosion
- Detonation of combustible gases
- Basemat penetration or containment bypass during Molten Corium Concrete Interaction (MCCI)
- Containment Overpressure (primarily due to long term loss of containment heat removal)
- Severe accident with containment bypass
- Significant fuel degradation in a storage fuel pool.

15.1.5 Analysis of Hazards

The analysis of hazards is captured in Sections 15.7 and 15.8.

15.1.6 Applicable Reference Documents

The general E3S design principles, approaches, methods, and requirements that govern the design to ensure the E3S fundamental objective can be met by the RR SMR are covered in E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [11].

The methodologies used for each safety analysis topic are referenced within the relevant sub-sections of this chapter.

15.1.7 Structure of Chapter 15

The chapter closely follows the structure that is set out by the IAEA for the safety analysis report. It follows the logical progression of safety analysis, which starts by fault and hazard identification and defining safety objectives and success criteria, followed by the various safety analyses that include deterministic and probabilistic analysis and hazard analysis. The section on deterministic analysis includes analysis of both DBCs and DECs. The approach to consideration of human actions is also described.

15.2 Identification, Categorisation and Grouping of Postulated Initiating Events and Accident Scenarios

15.2.1 Methodology and Scope

15.2.1.1 Overview

In order to demonstrate that all design basis faults are protected at all levels of DiD, the design basis and beyond-design basis faults are identified. These are faults which lead to a release of radioactive material or dose exposure to personnel, and which have a frequency of 1E-07 /yr or higher.

To identify these faults, a bottom-up approach is used, complemented by a top-down approach. The bottom-up approach uses hazard identification techniques to investigate each aspect of an SSC, which identifies the hazards present. These are then collated into a list of faults, through the process discussed in the following section. The top-down approach is a review of industry guidance and RGP, to ensure that all credible Pressurised Water Reactor (PWR) faults have been captured.

In this context, "hazards" refers to events which could threaten the correct operation of the system and delivery of the FSFs. The list of faults includes internally induced faults, termed "internal hazards", and hazards which originate from outside the site boundary, termed "external hazards". These and other definitions are covered in the E3S Principles [5].

15.2.1.2 Methodology

The methodology for identifying hazards, identifying initiating events and categorising these has been developed to ensure that there are structured techniques being used, and a structured process of grouping, to ensure that all foreseeable hazards and faults are identified. The cross-checks against other sources, discussed in this section, provide confidence in the list of identified faults and hazards.

Hazard identification exercises are carried out on the design and operations, in line with the Hazard Identification Strategy [13]. These include SWIFT, HAZOP studies (HAZOP1 and HAZOP2, depending on design maturity of the SSC), FMEA and others. Internal and External hazards are identified through specific techniques as discussed in the Hazard Identification and Analysis Company Standards [14] [15].

Hazards identified through these exercises number in the thousands and are collated in the Hazard Log [16]. The Hazard Log at DRP 1 has identified 501 hazards, distilled from 50 separate Hazard Identification studies. The individual records are referenced from the Hazard Log [16].

The Hazard Log provides a qualitative sentencing of the faults to determine whether they are credible fault initiators that could, if unmitigated, lead to a release of radioactive material or dose exposure to personnel. This sentencing is based on qualitative arguments, with justification and/or references presented.

Future work on the hazard identification task will include a wider scope of inputs to include hazard identification related to other disciplines such as C&I, cyber security and conventional health and safety inputs. The Hazard Log sentencing process will identify fault initiators which are required to be passed off to those areas of the E3S case for due consideration.

The faults/hazards which are sentenced for inclusion in the DSA (those which could lead to radiological or dose consequences and loss of FSFs) are carried forward into the PIE Definition exercise. The hazards are grouped as discussed in the following sections. The PIE Definition process undertakes a further step of grouping the hazards into PIEs, cross-checks the list of PIEs against industry guidance and RGP, including OPEX, to ensure completeness, and defines IEFs for the PIEs.

The IEFs are best estimate and are shared between the DSA and the PSA. The IEFs are derived from operating experience where available, as discussed in the PIE Definition report [17]. There are some instances where operating experience is not available, and so conservative estimations have been used, informed by available data and engineering judgement. Future work is planned to continue to refine these IEFs.

15.2.2 Basis for categorization of postulated initiating events and accident scenarios

The E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [11], sets out – at the highest level – how the PIEs and fault sequences relate to plant states and success criteria. Using that information, the PIEs are then characterised according to their IEF into the following categories:

- Normal operational expected events: have an IEF of more than 1E-2 /yr
- Frequent faults: have an IEF of more than 1E-3 /yr
- Infrequent faults: have an IEF between 1E-3 /yr and 1E-5/yr
- Beyond-design basis faults: have an IEF less than 1E-5 /yr.

Note that these categories apply to the PIEs, not to the fault sequences

This information is then used to categorize the fault sequences into the relevant DBC or DEC plant state and related acceptance criteria as explained in section 15.3.1 below.

15.2.3 Grouping of Design Basis PIEs

The design basis PIEs have been grouped into eight top level categories based on the nature of the fault. Further detailed groupings are applied within each category. Grouping and bounding is carried out by considering not only similar fault progression but also the severity of the fault, and the claimed safety measures.

The eight categories for the RR SMR are:

- ICF – These are faults which may lead to fuel melt but where the RCS and connected systems remain intact.
- Loss of electrical supply faults - These are faults which are defined by a loss of electrical supply to multiple systems which, if unmitigated, may cause the simultaneous failure of multiple systems.
- LOCA – These are faults which are defined by a loss of primary coolant from the RCS or connected systems.

- Fuel route & mechanical handling faults – These are faults which relate to the failure of mechanical handling equipment in containment and in the SFP.
- Spent fuel faults – These are faults are related to the SFP systems and include intact circuit failures and loss of SFP coolant faults.
- Internal hazards – These faults are defined as hazards that originate within the defined site boundary. For further detail see Section 15.7.
- External hazards – These faults are defined as hazards that originate outside the defined site boundary. For further detail see 15.8.
- Non-fuel melt faults – These are non-reactor faults which lead to operator, or off-site, radiological dose but not fuel melt.

The above categories are further decomposed to present more detailed bounding groupings. The next level of categories is shown in the table below.

Table 15.2-1: PIE Categories

Category	Grouping PIE ID	Grouping Description	PIEs in Group	Reference to Analysis Summary in Sections 15.5.3 to 15.5.8
Intact Circuit Faults	ICF.1	Primary flow-related faults	4	15.5.3.2 Analysis of Core Cooling and System Pressure for a Decrease of Reactor Coolant Flow
	ICF.2	Pressure-related faults	6	15.5.3.3 Analysis of System Pressure for an Increase of Reactor Coolant Inventory
	ICF.3	Reactivity-related faults	10	15.5.3.1 Analysis of Core Cooling and System Pressure for Reactivity-Induced Accidents
	ICF.4	Feed-related faults	5	15.5.3.5 Analysis of Core Cooling and System Pressure for a Decrease of Heat Removal by the Secondary Circuit
	ICF.5	Heatsink-related faults	8	15.5.3.4 Analysis of Core Cooling and System Pressure for an Increase of Heat Removal by the Secondary Circuit 15.5.3.5 Analysis of Core Cooling and System Pressure for a Decrease of Heat Removal by the Secondary Circuit 15.5.3.10 Analysis of Pressure–Temperature Transients in the Containment
Loss of Electrics	LOE.1	LOOP	2	15.5.3.6 Analysis of Loss of Electrical Power Supply
	LOC.0	Operator Exposure LOCAs	2	15.5.8 Analysis of Radioactive Releases

Category	Grouping PIE ID	Grouping Description	PIEs in Group	Reference to Analysis Summary in Sections 15.5.3 to 15.5.8
Loss of Coolant Accidents	LOC.1	Small LOCAs	2	15.5.3.7 Analysis of Core Cooling for Loss of Coolant Accidents (including Control Rod ejection fault) 15.5.3.8 Analysis of Primary Circuit to Secondary Circuit Leakage 15.5.3.10 Analysis of Pressure–Temperature Transients in the Containment
	LOC.2	Intermediate LOCAs	8	
	LOC.3	Large LOCAs	2	
Fuel handling	REF.0	General Mechanical Handling Faults	4	15.5.7 Analysis of Fuel Handling Faults
	REF.1	MOC Faults	18	
	REF.2	In Containment Fuel Handling Machine (FHM) Faults	19	
	REF.3	SPF FHM Faults	19	
	REF.4	Other Fuel Handling Faults	17	
Spent Fuel Pool	SFP.1	SFP ICFs	1	15.5.6 Analysis of Spent Fuel Pool Faults
	SFP.2	SFP LOCAs	7	
Internal hazards	INT.1	Reactor Island (RI) Internal Hazards	21	15.7 Internal Hazard Analysis
	INT.2	Non-RI Internal Hazards	4	
External hazards	EXT.0	External Hazards	8	15.8 External Hazards Analysis
Non-fuel melt faults	NFM.0	General Operator Exposure	1	15.5.8 Analysis of Radioactive Releases
	NFM.1	Waste Processing Faults	10	

15.2.4 List of Postulated Initiating Events and Accident Sequences

15.2.4.1 DBC Conditions

At the RD7/DRP1 design stage, a total of 178 PIEs have been identified as applicable to the RR SMR design. The PIEs are used as the basis for both the deterministic and the probabilistic safety assessment.

The full list of applicable PIEs is presented in Appendix B (section 15.12).

15.2.4.2 DEC-A Conditions

Analysis of DEC-A conditions is carried out to demonstrate that accidents that are more severe than the design basis, or involve additional failures, are covered in the E3S case. This ensures that there are no cliff-edge effects just beyond the design basis.

DEC-A sequences will be identified through examination of the fault schedule and the PSA, and by identifying sequences where the unmitigated consequences could lead to core damage or early release. The list of DEC-A sequences will be grouped where possible and will be reviewed against RGP. It is expected that some sequences identified as DEC-A as part of international RGP will be covered by DBC-4 analysis, which applies a more conservative approach. These sequences will not be repeated for DEC-A analysis.

The starting point for analysis of DEC-A sequences will be the closest equivalent Design Basis (DB) fault analysis. It is expected that codes and calculation tools for the analysis will be unchanged from DB analysis, but method changes will be applied.

For some sequences it is expected that the analysis with DEC-A methodology will provide evidence to show avoidance of large radiological release and no further design development will be required.

Where analysis indicates that a sequence or group of sequences is likely to result in significant core damage or early radioactive release then reasonably practicable provisions will be identified that can be implemented to reduce and/or delay the release.

The next version of the E3S case will contain more information on the identified DEC-A sequences and the analysis carried out.

15.2.4.3 DEC-B Accident Conditions

The end state of DEC-B sequences is reached through combinations of failures within the design basis measures or procedures which result in the progression of an accident sequence resulting in core melt (DEC-B). These sequences are of low probability.

The approach for the RR SMR taken at RD6 (and used to inform the safety case at DRP1) is informed by RGP and utilises engineering judgement to select three base case scenarios. The scenarios, although generic in nature, are deemed to be reasonably bounding of future entries into the PSA and allow for the assessment of a wide range of accident progression features [18]. Given the maturity of the design, the analysis is being conducted using limited scope and appropriate conservatism to limit risk to the project. The following three base cases for modelling are selected as follows:

- Large Break Loss of Coolant Accident (LBLOCA) with failure of all duty heat removal systems
- Slow depressurisation
- SBO.

Following on from the base case scenario selection, sensitivity cases are identified and analysed. The purpose of these cases is to provide further scrutiny to the performance of the severe accident mitigative measures (which form part of the CSM [JM01] v4 safety measure) during expected DEC-B conditions, with the aim of finding limiting conditions. Sensitivity studies are identified to reduce uncertainty in the analysis and to identify cliff edge effects. Scenario selection rationale is discussed in Section 15.5.5.6, for more detail see [18].

15.2.4.4 List of Internal and External Hazards

The list of Internal and External Hazards applicable to the RR SMR are presented in Sections 15.7 and 15.8.

15.2.5 Fault Schedule

The Fault Schedule aims to demonstrate that all design basis faults are adequately protected in line with the E3S principles and the categorisation and classification methodology. At version 2 of the E3S case, this is demonstrated for ICFs and LOCAs, and confidence is provided for other fault types such as handling, SFP and waste.

The Fault Schedule at the current version shows that safety functions are available for all identified ICF and LOCA PIEs. Work is ongoing to identify safety functions for other PIE categories – there are not expected to be any shortfalls in this area as the Fault Schedule is being used as a tool to inform the design through the identification of required safety functions.

The PIEs to be carried forward into the deterministic assessment are listed in the Fault Schedule [19]. The fault analysis presented in the Fault Schedule demonstrates clear and traceable linking of PIEs, fault sequences and the safety measures that provide DiD against postulated radiological consequences. Further information on the Fault Schedule development is presented in the DSA Methodology [20].

There are several future work items identified for the Fault Schedule, many of which reflect the evolving and maturing design, as described in Section 15.0; in particular the claimed safety measures for faults concerning shutdown operations, the SFP, mechanical handling (cranes) and waste systems need maturing. The Fault Schedule will be updated following DRP2 (RD8 design maturity gate) to reflect increased maturity and the ongoing design development and design decisions.

15.2.6 Environment, Safety, Security and Safeguards Requirements

The Fault Schedule [19] identifies DiD safety functions at each level against each FSF. The Fault Schedule then identifies sequences, which define the safety functions which need to act together to provide the protection against all FSFs together. The Safety Measures module [21] of the Fault Schedule suite of documents presents the safety measures which deliver the safety functions.

The Fault Schedule is also the tool for determining the nuclear safety categorisation, where the safety functions are assigned a categorisation which is flowed out in the form of classification of the safety measures.

The Fault Schedule is held and managed in the RR SMR requirements management database and can be exported to Excel spreadsheet format for the convenience of the user. The management of the Fault Schedule in the requirements management database enables the use of links to trace safety requirements and categories from the Fault Schedule via safety measures to SSCs.

The safety measure modules then flow down classified requirements to all of the necessary SSC which act together to deliver the safety measures.

For example, requirements are placed on the Category A Scram function to provide reactivity control against most design basis faults in Modes 1 and 2. Functional requirements are placed on the Class 1 Scram [JD01] safety measure to deliver these functions. The Scram [JD01] measure then places requirements on the Control Rods, Control Rod Drive Mechanisms (CRDMs), Reactor

Protection System (RPS) and other equipment to deliver the functions. Requirements are then flowed to sub-systems and components as required to support these.

This flow of requirements is held and managed in the RR SMR requirements management database and is discussed in the Safety Measure Design Descriptions (SMDDs) for the safety systems.

The current version of the E3S case includes these requirements for the headline safety systems which act to protect against ICFs and LOCAs. There is ongoing work to define and link the requirements on safety systems which support shutdown faults, the SFP, mechanical handling and waste systems.

15.2.7 Deterministic Safety Assessment informing the Design

The DSA provides a number of key routes for developing an E3S-informed design.

At the beginning of the DSA process, the hazard identification exercises provide a tool for the identification of optimisations which could be made to the design of specific SSC, particularly in relation to the safety of the plant.

The Fault Schedule identifies the available DiD and provides an important route for the deterministic safety case to inform the design, to identify any shortfalls in the provision of DiD, and the delivery of the functions claimed.

The following sections provide an overview of the analysis that has been carried out. The Design Basis Deterministic Safety Summary Report [22] provides further detail, drawing upon the Reactor Plant Performance Fault Study Analysis Summary [23]. These summaries, and the overview in this chapter, include discussion on instances where the output of the analysis has identified the potential for optimisation of the design, for example confirming where further claims could be made. Deterministic analysis also informs the setting of design limits, trip levels and equipment sizing.

15.2.7.1 Defence-in-Depth

Safety measures that deliver safety functions are defined in the fault schedule, and requirements on the safety measures are placed through links in the RR SMR requirements management database. The safety measures call upon a number of SSC to act together to deliver the safety measure. In some instances, the same SSC across the plant may be demanded by more than one safety measure to act at different levels of DiD as a fault sequence progresses. Therefore, there are instances where failure of a level of DiD may be assumed, and a demand will be placed upon the next level of DiD, but some SSC demanded in the first may also be required in the second.

A system-level discussion and justification of this is provided in the SMDDs, with reference to relevant decision files. The SMDDs place requirements on the equipment required to deliver the safety measures. Additionally, the ALARP Report [24] provides discussion on diversity for the key safety measures. The discussion below summarises, at a holistic plant level, key areas where this sharing of equipment across levels of DiD occurs, and where the justification is presented in the E3S case.

1. Local Ultimate Heat Sink (LUHS) [JNK] Tank Volumes (PDHR, ECC, In-Vessel Retention (IVR))

- A number of the headline heat removal safety measures (PDHR [JN02], ECC [JN01], IVR [JNM]) principally rely on the passive LUHS [JNK] as its heatsink, and yet substantial diversity of heatsinks is provided over the typical fault and accident sequence where these safety measures may be called upon. Notably, active Steam Generator (SG) cooling via Condenser Decay Heat Removal (CDHR) and Atmospheric Steam Dump (ASD) are diverse active safety measures in terms of their reliance on LUHS, whose functionality provides independent means to prevent core melt. Furthermore, IVR has both passive and active variants, only the passive variant demands LUHS, whereas the active variant can use Cold Shutdown Cooling System (CSCS) as a water source. Therefore, the heatsink estate over such a sequence includes four diverse heatsinks:

  - CDHR. Active safety measure utilising the duty heatsink for normal condenser heat removal via the Main Cooling Water System (MCWS) [PA] Mechanical Draft Cooling Towers.
  - ASD. Active safety measure dumping steam to the atmosphere via the SG relief system [LBK] with pumped inflow to the steam generators from water storage tanks using the emergency feedwater supply system [LJ].
  - PDHR. Passive heat rejection via the LUHS [JNK].
  - ECC. Passive heat rejection via the LUHS [JNK].
  - IVR. Passive heat rejection via the LUHS [JNK] or alternatively with the active variant utilising the essential service cooling water system [PB] cooling towers.

- Discussion on the sharing of heatsinks in this way is presented in the ALARP and Best Available Techniques (BAT) Position Paper on Reactor Heatsinks [25]. This investigated five options for the provision of heatsinks and the selected option was chosen on the basis that it is in keeping with guidance and practice and has a high likelihood of being reasonably practicable to implement.

2. Use of RCS [JE] for heat removal

- The ECC [JN01] and PDHR [JN02] functions both make use of the RCS [JE] to support the heat removal function. PDHR [JN02] uses SG cooling, through pumped or natural circulation flow within the RCS [JE] loops and heat transfer through the SG tubes to a secondary coolant. ECC [JN01] removes heat through Reactor Pressure Vessel (RPV) flood-up and boil-off into the containment atmosphere. Therefore, each safety measure relies on different heat transfer mechanisms: PDHR [JN02] uses pressurised reactor coolant flow through the core and SG to provide heat transfer; ECC [JN01] uses depressurised reactor coolant boiling.

- The RCS [JE] delivers category A safety functions, and so the SG, Reactor Coolant Pump (RCP) hydraulic casing and other pressure-retaining components, large bore pipework, pressuriser vessel and pressure relief valves are all designed to Class 1. The SG shell and tubesheet, secondary pressure-retaining components, RCP hydraulic casing and pressuriser vessel are Very High Reliability (VHR) components. More detail is presented in the System Design Description (SDD) for RCS [JE] [26].

3. Main Steam Isolation Valves (MSIVs)

- PDHR [JN02] requires steam isolation to provide closed-loop Passive Steam Condensing System (PSCS) [JNB] cooling of the SGs, and ECC [JN01] requires steam isolation to provide containment isolation. This involves sharing of equipment and does not meet the single failure criterion.

- There is RGP to support the use of a single MSIV per steam line; a decision record is currently being produced to investigate that this is ALARP.

4. Refuelling Pool [FAF]

- The High-Pressure Injection System (HPIS) [JND] draws water from the Refuelling Pool [FAF] in support of PDHR [JN02]; ECC [JN01] requires the Refuelling Pool [FAF] inventory to drain into the containment sump to support reactor heat removal.

- The Refuelling Pool [FAF] is a structure with high reliability claims on its structural integrity. Failure that leads to leaks would either be within the capacity of the HPIS [JND] recirculation pumps which would be able to maintain adequate Refuelling Pool [FAF] inventory in support of PDHR [JN02] or, if the leak was larger than the HPIS [JND] recirculation pump capacity, the SSC would fail to a safe state. Structural failure of the Refuelling Pool [FAF] would result in containment flood up; however, the HPIS [JND] suction line would remain sufficiently submerged to continue to operate with the Refuelling Pool [FAF] in this failed state.

5. HPIS

- The HPIS [JND] supports both the PDHR [JN02] and ASF [JD02], as well as providing inventory and pressure control for Low Temperature Decay Heat Removal (LTDHR) v2 (faulted CSCS cooling). This sharing of equipment is accepted on the basis that PDHR [JN02] supports delivery of Control of Fuel Temperature (CoFT) and ASF [JD02] supports delivery of Control of Reactivity (CoR).

6. Component Cooling System (CCS) & Essential Service Water System (ESWS)

- The CCS and ESWS cooling chain support PDHR [JN02] and ASF[JD02] as it cools the HPIS pumps and supports cooling for LTDHR and the Fuel Pool Cooling System (FPCS).

7. Electrical Power

- Standby Alternating Current (AC) power is demanded in the event of a loss of grid power to support ASF [JD02], and PDHR [JN02]. However, it is noted that the PDHR safety measure has configurations that can provide adequate CoFT without availability of the Standby AC power.

8. SFP

- The design of the SFP safety measures is being developed and the identification and justification of any sharing of SSC is a future work item.

15.3 Safety Objectives and Acceptance Criteria

15.3.1 Deterministic Safety Analysis Acceptance Criteria

E3S Case Tier 1 Chapter 3: E3S Objective & Design Rules [11] sets out, at the highest level, how the DiD levels relate to plant states and success criteria. Using that information, the Fault Schedule [19] links every fault sequence to its applicable plant state and therefore to a set of success criteria. The top-level success criteria are typically described as breaches in barriers, which is decomposed in line with the EUR and other RGP as follows:

Table 15.3-1: Deterministic Success Criteria

<table>
<tr><th>Plant States and meaning</th><th>Success criterion</th><th>First barrier:
Fuel and cladding</th><th>Second barrier:
RCS</th><th>Third barrier:
Containment</th></tr>
<tr><td colspan="2">Based on E3S Case Tier 1 Chapter 3: E3S Objectives & Design Rules for SSCs [11]</td><td>Based on SMR0005456 [27]</td><td></td><td></td></tr>
<tr><td>DBC-2ii and DBC-3i: frequent faults with first line of protection</td><td>No physical barriers breached where reasonably practicable</td><td>No fuel failures, decomposed into:
- ICFs: No Departure for Nucleate Boiling (DNB)
- DHR: no sustained voidage in the upper plenum
- Maximum clad temperature
- No fuel melt: Maximum fuel temperature</td><td>RCS remains intact where reasonably practicable
- Maximum RCS design pressure and temperature</td><td rowspan="3">Containment remains intact, decomposed into:
- Maximum containment design pressure 0.685 MPa and temperature 164°C</td></tr>
<tr><td>DBC-3ii: infrequent faults with IEF > 1E-04 /yr</td><td rowspan="3">No more than limited relocation of radioactive material confined by at least one physical barrier (i.e. fuel clad, RCS, containment)</td><td rowspan="2">Interpreted as “maintain coolable geometry”, decomposed into:
- <u>ICFs</u>: Maximum 5% (DBC-3ii) / 10% (DBC-4) clad failures due to DNB
- <u>ICFs and LOCA</u> (including use of ECC):
o Limits on clad temperature and clad oxidation
o No fuel melt: Maximum fuel temperature</td><td rowspan="2">N/A</td></tr>
<tr><td>DBC-4: infrequent faults with IEF < 1E-04 /yr, or frequent faults with second line of protection</td></tr>
<tr><td>DEC-A: beyond-</td><td colspan="3">The success criteria are identical to DBC-4, but assessed using best-estimate rather than conservative methods</td></tr>
</table>

Plant States and meaning	**Success criterion**	**First barrier: Fuel and cladding**	**Second barrier: RCS**	**Third barrier: Containment**
design-basis faults with IEF < 1E-05 /yr, or sequences more complex than DBC-4				
DEC-B: controlled severe accidents	At least one physical barrier intact confining any substantial relocation of radioactive material	Fuel melt is accepted, but corium is confined in RPV.	RCS is depressurised. The RPV [JAA] shall remain intact and contain the molten corium. The predicted heat flux on the RPV outside is lower than the Critical Heat Flux (CHF)	**Containment remains intact**, decomposed into [18]: The containment pressure shall not exceed 0.7 MPa(a)[2]. The global average hydrogen concentration within containment shall not exceed more than 10 % by volume in dry air or 13 % in steam.
Beyond DEC-B	Large and early release	In the deterministic assessment, this is only modelled as "unmitigated consequences", but these sequences are modelled in the PSA outcomes		

The Fault Schedule [19] then links each sequence to its pertaining plant state and, therefore, to a success criterion. These criteria are then used as safety limits in the performance analysis.

Note that the table above only shows selected key criteria. Further detail is provided in the Justification of Design Limits document [27] for fuel safety limits, and in [JM01] SMDD [28] for containment.

For some faults, in particular for SGTR, where containment is bypassed as part of the IEF, the radiological safety limits as specified in E3S Case Tier 1 Chapter 3: E3S Objective & Design Rules [11] are also assessed directly.

15.3.2 Probabilistic Safety Assessment Acceptance Criteria

The Tier 1 Chapter 3 of this E3S case sets out the acceptance criteria and RR SMR Numerical Targets for the design. These are based on the Basic Safety Levels (BSLs) and Basic Safety Objectives (BSOs) in the ONR SAPs Targets 1 – 9 and align with international guidance and practices. Noting that doses and risks must be always controlled and reduced to ALARP irrespective of whether numerical targets

[2] This pressure value has been derived from the maximum permissible hoop stress calculated in accordance with ASME III NE for design basis analysis but without additional conservatism applied for variation in atmospheric conditions or to account for additional uncertainty. A higher pressure, termed the Containment Vessel Ultimate Pressure Capacity, based on yield strength, may be used as the acceptance criteria for future assessments of limiting scenarios.

have been achieved, the acceptance criteria for the RR SMR design that are supported by the development and use of the PSA are identified as:

Table 15.3-2: RR SMR Numerical Targets (replicated from [5])

Metric	Plant State	Shall be lower than	Should be lower than	Basis
Individual risk of death to a person on the site from accidents at the site resulting in exposure to ionising radiation	Accident Conditions	1E-04 pa	1E-06 pa	ONR SAPs Target 5 BSL and BSO [29]
The predicted frequency of any single accident giving an effective dose to any person on-site, of: 2-20 mSv 20-200 mSv 200-2000 mSv >2000 mSv		1E-01 pa 1E-02 pa 1E-03 pa 1E-04 pa	1E-03 pa 1E-04 pa 1E-05 pa 1E-06 pa	ONR SAPs Target 6 BSLs and BSOs [29]
Individual risk of death to a person off the site from accidents at the site resulting in exposure to ionising radiation		1E-04 pa	1E-06 pa	ONR SAPs Target 7 BSL and BSO [29]
The predicted frequency of accidents giving an effective dose to any person off-site, of: 0.1-1 mSv 1-10 mSv 10-100 mSv 100-1000 mSv >1000 mSv		1 pa 1E-01 pa 1E-02 pa 1E-03 pa 1E-04 pa	1E-02 pa 1E-03 pa 1E-04 pa 1E-05 pa 1E-06 pa	ONR SAPs Target 8 BSLs and BSOs [29]ONR SAPs Target 8 BSLs and BSOs [29]
The total risk of 100 or more fatalities from accidents at the site resulting in exposure to ionising radiation		1E-05 pa	1E-07 pa	ONR SAPs Target 9 BSL and BSO [29]
Core Damage Frequency		1E-05 pa	1E-07 pa	EUR [30] INSAG-12 [31] NRC [32]
Large or Early Release Frequency		1E-06 pa	1E-08 pa	EUR [30] NRC [32]
†: Definitions of these terms can be found in Appendix 4 of the E3S Design Principles [5].				

The PSA provides quantitative assessment of the design and plant operation to derive numerical values that can be compared against these targets. The Level 1 PSA is used to determine the CDF. The Level 2 PSA is used to determine the Large or Early Release Frequency in collaboration with the Severe Accidents topic. The Level 3 PSA is used to determine the frequency of radiation exposure from accidents to individuals on-site, individuals off-site and the wider population, in collaboration with the Radiological Consequences topic. Consideration of the results of the PSA against these metrics is covered in Subsections 15.6.2, 15.6.3 and 15.6.4.

15.4 Human Actions

15.4.1 General Considerations

A key design principle of the RR SMR is for systems to be passive or automated where practicable, which limits claims on the operator. Similarly, there is an expectation that the SMR will be 'secure by design' to limit the need for active security systems and associated security-based claims on the operators. The RR SMR is a PWR, with few areas of novelty in its operation. Where novel areas exist, the opportunity to reduce the reliance on operators has been taken, for example through reducing the number of normal operational discharges to manage.

Whilst increased passivity will be provided against all modes of operation, operator actions are still required to perform a number of normal operational duties during power and shutdown operations, monitor the initiation of safety systems, and contribute to the longer-term management of safety systems and emergency arrangements.

Operator actions will be identified through a number of sources, including HAZOP studies, Fault Schedule, PSA, SDDs, Examination, Maintenance, Inspection, and Testing (EMIT) activities as defined in the Through Life Activity (TLA) module of the RR SMR requirements management database, and the decomposition of operator activities via task analysis. Given the concept maturity, the identification of operator actions is still progressing.

Further detail is provided in Chapter 18 [33].

15.4.2 Human Actions in Deterministic Safety Analysis

For the DSA carried out to date there are no claims on the operator to initiate Category A or B protective safety functions, with the possible exception of initiation of a response to SGTR, for which it is currently being reviewed to determine whether it can be automated. This is a result of a key design principle of the RR SMR for systems to be passive or automated, which limits claims on the operator. There are, however, claims on the operator to support the long-term success of Category A and B protective safety functions, including topping up LUHS and diesel oil fuel tanks after the required time.

There are a number of claims on the operator to initiate preventive safety functions, including manual scram, and in the prevention of pressure related PIEs, such as pressuriser heater actuation, Chemical and Volume Control System (CVCS) stop and pressuriser spray trip. All operator initiated preventive safety functions are category C and are backed up with automated protective safety functions should the operator fail to complete the action.

The majority of plant faults place a claim on the Severe Accident Containment safety function, which includes operator initiation of IVR. This is a Category C function, where operator initiation is supported by relevant OPEX due to the requirement for consideration of multiple factors prior to the decision to initiate the function.

All safety functions claimed in response to a fault that are initiated by and/or require long term support from the operator have associated Human Based Safety Claims (HBSC). These have been derived by the Human Factors (HF) team from the Fault Schedule and the operating philosophies for each safety function.

It is anticipated that further operator actions required will be identified through development of the deterministic safety case (HAZOPs, Fault Schedule), resulting in additional HBSCs. HBSC substantiation is owned by HF, with further detail provided in Chapter 18.

15.4.3 Human Actions in Probabilistic Safety Assessment

The RR SMR PSA includes numerous operator actions, which are identified as part of the modelling process, primarily via the event sequence modelling activities and the SSC modelling activities. In most cases these PSA-identified operator actions are directly associated to a particular HBSC as derived from the Fault Schedule. In addition, new operator actions were added and claimed in the PSA model, as these were considered best practice from a probabilistic perspective. Such additional operator actions have been shared with HF for the derivation of additional, associated HBSC. As a safety analysis topic, the scope of operator actions in the RR SMR PSA excludes any malicious action taken with deliberate intent.

Currently, there is insufficient qualitative evidence available to derive best-estimate values for Human Error Probabilities (HEP). Therefore, an early approach on HEP values for the RR SMR PSA was agreed by the PSA and HF teams, where the current PSA model applies a HEP of 1.00E-02 to all operator actions within the RR SMR PSA. This value is assumed to represent the current best estimate given the insufficient input data available for assessment and substantiation of HBSC from which qualitative evidence is drawn from to derive more accurate HEP. Other screening value approaches were considered and rejected as being less representative. Additionally, the PSA assumes that Human-Machine Interfaces (HMIs) are perfectly reliable, and that the locations are perfectly suited to perform any claimed operator action.

It is acknowledged that while this approach will not provide best estimate results until the design matures further, it currently allows a risk ranking of the operator actions within the PSA, to support prioritisation of further analysis and HF engineering input. As per the PSA Technical Requirements [34], sensitivity studies were performed on the HEPs of each operator action, to identify scenarios where human actions claimed within the PSA are particularly of interest. As the design matures, a more detailed approach will be taken on these operator actions, such as the use of Human Reliability Assessments.

15.5 Deterministic Safety Analysis

15.5.1 Deterministic Analysis General Approach

15.5.1.1 Conservatism in Safety Analysis

The design basis DSA aims to demonstrate that the safety criteria are met with a high confidence level. The Design Basis methodology is set of procedures and guidance for the analysis studies to be carried out in a manner that ensures the conservative nature of the results. The methodology uses calculation codes which are supported by Verification, Validation and Uncertainty Quantification (VVUQ) demonstrating they are appropriate for their modelling applications.

The design basis deterministic performance analysis methodology [35] has been developed following consultation of the following guidance and technical reporting – the Performance Methodology report [35] discusses which aspects of this guidance has been applied in the methodology, noting that there are differences and potentially conflicts between the listed sources.

- Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles [11]
- The ONR SAPs and relevant TAGs on Design Basis Analysis
- IAEA Safety Standard - Deterministic Safety Analysis for Nuclear Power Plants – Specific Safety Guide (SSG-2) – Revision 1 [36]
- European Utilities Requirements (EURs) on Light Water Reactor Safety [30] [37] [38]
- United States Nuclear Regulatory Commission, “10 CFR Parts 50 and 52 Performance-Based Emergency Core Cooling Systems Cladding Acceptance Criteria [39]
- United States Nuclear Regulatory Commission, “10 CFR § 50.46 Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors [40]
- The Advanced Passive 1000 MW_e Pressurised Water Reactor (AP1000) Pre-Construction Safety Report (PCSR) [41] and the ONR GDA Step 4 assessments of Design Basis faults [42]
- The European Pressurised Water Reactor (EPR) PCSR sub-chapters on assumptions and requirements for the plant condition categories accident analyses [43], risk reduction analysis [44], and the ONR GDA Step 4 assessments of Design Basis faults [45].

The design basis analysis methodology for each accident scenario is developed in several stages:

1. Accident initiating event definition.
2. The plant response is reviewed, the dominant physical phenomena are identified and the acceptance criteria are determined. An appropriate analysis code or set of analysis codes for modelling the plant response is then defined.
3. A combined approach is used to manage uncertainties in the design basis analysis. The combined approach ensures overall conservatism of the analysis results by using best-estimate physical models and conservative initial and boundary conditions and SSC availability.

4. The initial and boundary conditions and SSC which have a dominant impact on the acceptance criteria are identified for each accident scenario. Uncertainties on these parameters are applied in a deterministic manner with each dominant parameter considered at its conservative value. At this methodology iteration, uncertainties in initial and boundary conditions are bounded with conservative values recognising the maturity of the design.

5. Sensitivity studies are used to help identify the bounding initial and boundary conditions, single failures and SSC availability.

The Design Basis Performance Methodology [35] discusses how the following considerations have been approached:

- Operating modes and plant states
- Initial plant conditions
- Power distribution
- Reactivity coefficients
- Boron reactivity coefficient
- Decay heat
- RCCA insertion
- C&I assumptions
- Operator actions
- Material properties
- Common cause failure (CCF)
- Consequential failure
- LOOP
- Preventive maintenance
- Safety measure availability
- Single failure
- Anticipated Transient Without Scram (ATWS)
- Grid frequency.

15.5.1.2 Computer Codes for DBC and DEC-A

The key codes used to model DBC and DEC-A scenarios are listed below with a short description of its purpose and reference to its validation summary.

- RELAP5-3D
    - A thermal hydraulic system code which is used to model the overall transient response of the primary and secondary circuit during normal operations and fault conditions. The code determines the evolution of the thermal hydraulic parameters around the systems during the scenario such as flow rate at a leak site or height of liquid volume within the core. This is the primary tool used in modelling normal operations, ICF, LOE and LOCA.
    - Validation is discussed in the Thermal Hydraulics VVUQ Summary [46].
- VIPRE-01
    - A thermal hydraulic sub-channel code which is used to model the flow and heat transfer behaviour within the core at a higher level of detail than in the system model, with resolution of individual fuel pins and flow channels. Used for calculating core and fuel parameters such as Departure for Nucleate Boiling Ratio (DNBR), pellet temperature, and cladding temperature.
    - Validation is discussed in the Thermal Hydraulics VVUQ Summary [46].
- GOTHIC
    - A thermal hydraulic system code which is used to model the containment pressure following a release from the primary or secondary circuit such as during a LOCA or MSLB.
    - Validation is discussed in the Thermal Hydraulics VVUQ Summary [46].
- CASMO5 and SIMULATE5
    - CASMO5 is a lattice physics code for PWR and heterogeneous fuel designs. SIMULATE5 builds upon this to model steady-state core neutronics. These codes are used in the core design and to derive physics input data and boundary conditions for the RELAP5-3D and SIMULATE5K codes.
    - Validation is discussed in the Reactor Physics Validation report [47].
- SIMULATE5K
    - SIMULATE5K is a tool built upon SIMULATE5 to model the transient 3D core response to reactivity faults where there is a strong coupling between core neutronics and thermal hydraulics. Input data for the overall transient plant response to a fault can be provided as an input to SIMULATE5K from RELAP5-3D.
    - Validation is discussed in the Reactor Physics Validation report [47].
- ADMS
    - The design basis radiological consequences analysis methodology identifies the use of ADMS to model the atmospheric dispersion and deposition of radioactive release. Validation of ADMS is discussed in the Design Basis Radiological Consequences Methodology [48].

15.5.2 Analysis of Normal Operation

The conduct of normal operations is discussed in Chapter 13 [1]. Chapter 16 [2] discusses OLCs for safe operation, which are informed by safety analysis as discussed in the Deterministic Safety Assessment Methodology [20]. In addition, some normal operation dose assessments have been carried out which are discussed in Chapter 12 [49].

Safety analysis informs OLCs through identification of safety limits or assumptions that are made in the performance analysis. For example, limits on shutdown margins and core reactivity will be translated into OLCs on normal operation. OLCs will be identified from the requirements and definitions defined in the RR SMR requirements management database against each system.

There is further work identified to derive a set of analysis-informed OLCs, this is discussed in Chapter 16 [2]. This includes DBC-2i conditions which are not faults, but deviations from normal operation.

15.5.3 Analysis of Design Basis Fault Conditions

The Design Basis Deterministic Safety Assessment Summary Report [22] provides an overview of each fault group analysed at the current stage. For each fault group, this presents a definition of the PIE, its frequency and consequences, a listing of the safety functions provided in the Fault Schedule and a list of the safety measures which deliver them, an overview of the means of initiation of the safety measures, discussion on any HBSCs and a summary of the analysis.

The subheadings below provide a higher level overview of the deterministic analysis of these design basis fault conditions, with a focus on demonstrating that the analysis shows that acceptance criteria are met.

The below list presents a subset of key faults applicable to power operation (Modes 1 and 2). The selected faults are bounding faults for which analysis has been performed to provide confidence in the ability of the plant to protect against most faults. The rationale for selection of these faults is discussed in the Reactor Plant Performance Fault Study Analysis Summary [23] and is summarised below.

- ICF.1.1.01: Complete Loss of Pumped Primary Flow
- ICF.1.1.03: RCP Shaft Seizure (Locked Rotor)
- ICF.3.2.03: Excessive Steam Demand due to Large Un-Isolable Steam Leak (a main steam line break)
- ICF.5.1.03: Turbine Trip
- The Station Blackout (SBO) elements of LOE.1.0.01: LOOP (72 hours)
- LOC.2.1.01: Intermediate Un-Isolable LOCA
- LOC.2.1.02: LOCA due to SGTR
- LOC.3.1.01: Large Un-Isolable LOCA.

The Loss of Flow faults were selected as bounding transients on the basis that the faults are potentially limiting for Scram [JD01] and ASF [JD02]. Due to the rapid reduction of flow through the core, these are assessed against core thermal limits.

The large un-isolable (upstream) steam leak (MSLB) is assessed as a potential bounding increase in heat sink transient as it imparts the largest cooldown rate of the reactor circuit temperature and, therefore, the largest potential increase in core reactivity prior to Scram [JD01] initiation.

The limiting Loss of Offsite Power assessed within the design basis is referred to as a "station blackout", which is defined as a Loss of Offsite Power followed by subsequent unavailability continuous AC power (via either the Main or standby generators). Station Blackout transient is assessed as a potentially limiting loss of heat sink transient that demonstrates the ability of PDHR [JN02] to remove the maximum decay heat for which is it claimed.

ECC [JN01] is required to automatically depressurise the reactor plant following an intermediate LOCA to enable accumulator injection and provide control of fuel temperature. As such, this fault is assessed as a potentially limiting case for ECC performance in terms of PCT, fuel clad oxidation.

A large break LOCA represents the fastest depressurisation fault and the most rapid demand on the initiation of ECC. As such, this fault is assessed as a potentially limiting case for ECC performance in terms of PCT, fuel clad oxidation, containment pressure and containment temperature.

15.5.3.1 Analysis of Core Cooling and System Pressure for Reactivity-Induced Accidents

This section covers analysis of the following PIEs:

- ICF.3.1.01: Spurious scram
- ICF.3.1.02: Reactivity control imbalance (dropped rod(s))
- ICF.3.1.03: Spurious initiation of ASF
- ICF.3.2.01: Excessive control rod bank withdrawal
- ICF.3.2.05: Temperature reduction of feedwater supply
- ICF.4.2.01: Excessive feedwater supply
- LOC.2.1.05: CRDM LOCA – leading to Rod Ejection (reactivity aspects only; noting that the LOCA aspects are covered in section 15.5.3.7).

Analysis for these faults is ongoing and will be reported in a future update of this chapter in Version 3 of the E3S case.

While analysis carried out gives confidence in the design, future work is identified to assess performance of Scram [JD01] and ASF [JD02] against these faults. Following successful reactor shutdown (via Scram or ASF), the maximum heat removal requirement on PDHR is bounded by a SBO which results in a faster plant temperature increase. The earliest time that ECC is required to initiate is bounded by the LBLOCA transient. As such, Peak Clad Temperature (PCT), clad oxidation and containment peak pressure are bounded by large and intermediate LOCA. Following safe shutdown via Scram, but failure of PDHR, the rate of plant temperature increase is bounded by SBO. As such, maximum depressurisation rate required by ECC following an ICF is bounded by SBO.

15.5.3.2 Analysis of Core Cooling and System Pressure for a Decrease of Reactor Coolant Flow

This grouping considers the following PIEs:

- ICF.1.1.01: Complete Loss of Pumped Primary Flow
- ICF.1.1.02: Partial or Recoverable Loss of Pumped Primary Flow
- ICF.1.1.03: RCP Shaft Seizure
- ICF.5.3.02: Recoverable Loss of Service Water (CCS, ESWS).

ICF.1.1.01, ICF.1.1.02 and ICF.5.3.02 cover a loss (coast down) of, respectively, all or some duty RCS pumps – in Modes 1-4A this is the RCPs and in Modes 4B-6A it is the CSCS pumps. Analysis has been conducted on at-power modes only, so only considers the RCPs. For ICF.5.3.02 note that the RCPs are cooled by CCS, and so loss of CCS may lead to loss of RCPs.

The loss of RCPs results in a core flow rate drop causing a reduction in heat removal from the fuel and primary coolant which leads to an increase in core temperature. If unmitigated, this will cause DNB, a rise of fuel and cladding temperatures, fuel melt, and radiological release.

ICF.1.1.03 is defined by an instantaneous seizure of the shaft of a single RCP giving a greater initial rate of reduction of coolant flow in comparison to ICF.1.1.01 & 02 as it is a 'hard stop' rather than an 'inertial coast down' of the affected pump. This results in a rapid reduction in flow in the affected loop causing a reduction in core heat removal and increasing fuel temperatures. This can lead to DNB, reducing heat removal further. If unmitigated, this will cause a rise of fuel and cladding temperatures, fuel melt, and radiological release.

The following sequences (in chronological order) have been analysed with the following success criteria:

- Fault with first line of protection: both complete loss of flow and pump seizure have been assessed, and pump seizure has been found to be the limiting transient for Scram, which is assessed against the criteria for plant state DBC-2ii, meaning no DNB.
- Fault with second line of protection: Sequences with failure of scram, which use ASF instead, have not yet been analysed.

Following safe shutdown (via scram or ASF) the decay heat removal aspects are bounded by a SBO, see section 15.5.3.6.

RELAP5-3D is used to model the plant response. Bounding conditions are then passed to VIPRE-01 to more accurately model the DNBR for the peak pin (for Scram).

Plant parameters are conservative. A starting reactor power of 102 % is used, and bounding assumptions are made for the local power of the peak pin. Conservative assumptions are used for RCP coast down curve and rod-insertion profile. Reactivity coefficients are also conservative.

For Scram, a single stuck rod is assumed. The most limiting RPS and Diverse Protection System (DPS) trips are modelled on the assumption of a single failure. Operator action is not required.

The loss of flow fault is identified very rapidly (<1 s). With Scram available, this results in shutdown of the reactor within 5 s of fault initiation. During the brief period between loss of power to the RCPs and Scram being effective, there is an increase in coolant temperature within the core. Even with pessimistic reactivity feedback effects considered in the modelling, this results in a significant reduction in reactivity due to moderator density reactivity feedback.

A good margin to DNBR limit has been demonstrated (as reported in the Analysis Summary [23]) for this fault when Scram is initiated on the RPS or the DPS trip.

Demonstration that containment remains intact if PDHR failed and ECC was needed is bounded by the assessment of MSLB or LBLOCA in sections 15.5.3.4 and 15.5.3.7. Assessment of radiological consequences outside of containment is ongoing.

Sensitivity studies have been carried out modelling all three PIEs individually, and also the LOOP scenario, which results in a similar fault progression. Furthermore, sensitivity studies were carried out to determine the most limiting trip parameter (as reported in the Analysis Summary [23]).

15.5.3.3 Analysis of System Pressure for an Increase of Reactor Coolant Inventory

Analysis for these faults is currently bounded by other fault groups. Analysis will be carried out and will be reported in the next update of this chapter.

15.5.3.4 Analysis of Core Cooling and System Pressure for an Increase of Heat Removal by the Secondary Circuit

This grouping considers the following PIEs:

- ICF.2.3.05: Temperature reduction of feedwater supply
- ICF.4.2.01: Excessive feedwater supply
- ICF.3.2.02: Excessive Steam Demand due to Large Isolable Steam Leak
- ICF.3.2.03: Excessive Steam Demand due to Large Unisolable Steam Leak (also known as Unisolable MSLB)
- ICF.5.2.01: Excessive Steam Demand due to Small Isolable Steam Leak
- ICF.5.2.02: Excessive Steam Demand due to Small Unisolable Steam Leak
- ICF.3.2.06: Excessive Steam Demand due to Spurious Steam Generator Relief Valve (SGRV) Lift
- ICF.3.2.07: Excessive Steam Demand due to Spurious ASD Activation
- ICF.4.1.04: Unisolable Feed Line Break (FLB) (short-term: increase in heat removal).

Analysis has so far been carried out for the bounding fault of unisolable MSLB, and for the other faults is ongoing and will be reported in the next update of this chapter.

ICF.3.2.03 covers failures downstream of the SG outlet nozzle and upstream of the MSIVs, which cannot be isolated and so the SG inventory is lost through the leak site. The most bounding case is a double-ended guillotine break of a main steam line (commonly referred to as an MSLB).

The unmitigated fault progression follows a rapid blowdown of all SGs to atmospheric pressure causing an increased steam flow through the SGs improving heat transfer. If unmitigated, this will rapidly lower the reactor temperature, causing a significant increase in reactivity. The sharp reactivity rise can lead to DNB, fuel melt, and a consequent radiological release.

The following sequences (in chronological order) have been analysed with the following success criteria:

- Fault with first line of protection: unisolable MSLB with Scram and PDHR is assessed as a DEC-A event (because in the deterministic sense PDHR is an "additional line of protection" for this infrequent fault), but in fact for conservatism is assessed against a criterion of no DNB (for scram) and the PDHR criterion of no sustained voidage in the upper plenum.

- Fault with second line of protection: the criteria for plant state DBC-3ii apply to the sequence unisolable MSLB with Scram and ECC. The ECC response has not been assessed but is considered to be bounded by LBLOCA.

Intact containment must also be demonstrated in both cases.

Note that consequential SGTR is not assumed on the basis that MSLB and FLB are load cases in the mechanical design of the SG tubes.

RELAP5-3D is used to model the plant response. Bounding conditions are then passed to VIPRE-01 to more accurately model the DNBR for the peak pin (for Scram). GOTHIC is used to model the containment pressure.

Plant parameters are conservative. A starting reactor power of 102 % is used, and bounding assumptions are made for the local power of the peak pin. Conservative assumptions are used for rod-insertion profile. Reactivity coefficients are also conservative. For Scram, a single stuck rod is assumed. The most limiting RPS and DPS trips are modelled on the assumption of a single failure.

The results demonstrate that the PCT acceptance criterion is met with margin. Compliance with the DNBR acceptance criterion is met with margin. As such, Scram is deemed an effective Control of Reactivity (CoR) measure for this limiting fault.

The PDHR safety measure was primarily assessed against its ability to maintain RCS and secondary pressure below design pressure conditions and maintain fuel PCT. The results demonstrate that under pessimistic boundary conditions with consequential RCP failure, all temperature and pressure criteria are met with ample margin. Thus, it is shown that PDHR is an effective means of RCS pressure control and heat removal during a bounding fault.

The results of the containment thermal analysis show that containment limits are met, see section 15.5.3.10 for results and discussion.

RCS and secondary pressure criteria were not expected to be challenged in this case and this was demonstrated. Assessment of radiological release is still ongoing for this limiting fault. The containment analysis that is discussed in the paragraph above demonstrates that containment remains intact even in the case of MSLB with ECC.

Sensitivity studies have been carried out modelling consequential loss of RCPs. Furthermore, sensitivity studies were carried out to determine the most limiting trip parameters (as reported in the Analysis Summary [23]).

15.5.3.5 Analysis of Core Cooling and System Pressure for a Decrease of Heat Removal by the Secondary Circuit

This grouping considers the following PIEs:

- ICF.4.1.02: Partial loss of SG feed
- ICF.4.1.03: Loss of duty SG feed
- ICF.4.1.04: Unisolable FLB (long-term: decrease in heat removal)
- ICF.5.1.01: Loss of Condenser
- ICF.5.1.02: Partial isolation of steam route to condenser
- **ICF.5.1.03: Turbine trip**
- ICF.5.1.04: SG isolation due to spurious PDHR
- ICF.5.1.06: Spurious containment isolation.

The **turbine trip** PIE has been assessed as a key fault that represents the other faults listed above. ICF.5.1.03 is an isolation of the steam route to the condenser following an unplanned trip of the turbine. It is assumed for the unmitigated sequence that there is no turbine bypass function and thus the turbine trip isolates the steam route to the condenser. This causes a loss of function of the secondary heatsink leading to a reduction in the heat removal from the RCS which, if unmitigated, will result in an increase in core temperature resulting in potential fuel melt and consequent radiological release.

The following sequences have been analysed with the following success criteria:

- Turbine trip with first line of protection (Scram and PDHR) is assessed against the criteria for plant state DBC-2ii, meaning no DNB (for scram) and the PDHR pseudo criterion of no sustained voidage in the upper plenum. This analysis has not yet been performed and will be reported in a future version of this chapter.
- Turbine trip with second line of protection:
    - A sequence with Scram and ECC is assessed against the criteria for plant state DBC-4; scram is still assessed against a criterion of no DNB, and ECC is assessed against the LOCA criteria of limits on clad temperature and clad oxidation. The containment aspects (following ECC) are bounded by that in the LBLOCA and MSLB analysis, see sections 15.5.3.7 and 15.5.3.4.
    - A sequence with failure of scram, which uses ASF instead, has not yet been assessed.

RELAP5-3D is used to model the plant response. Turbine trip is only assessed against the primary and secondary pressure criteria; the DNBR assessment is bounded by Complete Loss of Flow (CLOF) studies, and the assessment of ECC is bounded by SBO.

Plant parameters are conservative. A starting reactor power of 102 % is used, and bounding assumptions are made for the local power of the peak pin. Conservative assumptions are used for rod-insertion profile. Reactivity coefficients are also conservative. For Scram, a single stuck rod is assumed. The most limiting RPS and DPS trips are modelled on the assumption of a single failure. Operator action is not required.

The analysis demonstrates that the Scram and ECC safety measures are effective at protecting the plant for a turbine trip assessed using bounding initial conditions and assumptions. Assessment of this limiting scenario with only ECC available provides confidence that there will be significant margins with other safety measures available.

The safety measures ensure that the reactor circuit and SG pressures are maintained with the design limits, there is significant margin to pressuriser overfill and the pressuriser Safety Relief Valves (SRVs) do not lift. Assessment of radiological release is still ongoing for this limiting fault. The containment analysis that is discussed in section 15.5.3.10 demonstrates that containment remains intact with ECC.

Sensitivity studies have been carried out modelling consequential LOOP. Furthermore, sensitivity studies were carried out to determine the most limiting trip parameters.

15.5.3.6 Analysis of Loss of Electrical Power Supply

This grouping considers the following PIEs:

- LOE.1.0.01: LOOP for 72 hours
- LOE.1.0.02: LOOP for 168 hours.

These faults cover failure of the main grid connection and any auxiliary connection to offsite power sources. Any on-site standby and alternate AC power supplies may be claimed as safety measures, as well as tripping to house load. For derivation of an IEF, discussions will be held with National Grid plc to review LOOP PIEs and ensure alignment between the Rolls-Royce SMR DSA & National Grid reliability estimates.

The fault sequences for these PIEs include SBO (which is covered in the Fault Schedule as a LOOP with failure of the first protective safety measure), but not onsite distribution failures.

In response to a LOOP, the plant would initially attempt a switchover to house load operation, with the reactor continuing to operate and onsite power being provided by the turbine. Failure to switchover to house load would result in a reactor trip on low RCP speed and the diesel generators would be activated as the first line of electrical backup protection to supply power to the decay heat removal systems.

Unmitigated, the fault progression causes all electrically powered systems to stop, including all pumps to coast down. This will cause a reduction in heat removal from the core due to the coast down of the RCPs reducing core flow, and the coast down of the feed pumps reducing SG heat removal. If unmitigated, primary and secondary circuit temperature and pressure will rise, eventually breaching safety limits, causing fuel overheating, eventual fuel melt and radiological release.

Loss of cooling to the SFP will be covered separately.

The following sequences have been analysed with the following success criteria:

- 72-hour LOOP with first line of protection (Scram and PDHR with HPIS powered by standby AC) is assessed against the criteria for plant state DBC-2ii, meaning no DNB (for scram); only the short term (scram-related) aspects of this particular sequence have been assessed as part of the CLOF study, because the focus of the SBO analysis was on the next sequence (PDHR with accumulators instead of HPIS).

- 72-hour LOOP with partial failure of first line of protection, i.e. with failure of standby AC, is also commonly known as SBO. It is assessed with Scram and PDHR with accumulators (without HPIS) as an “additional” line of protection in the deterministic sense, i.e. as a DEC-A scenario. Conservatively the same assessment criteria are applied, i.e. no DNB (for scram – assessed as part of the CLOF study) and the pseudo criterion of no sustained voidage in the upper plenum (for PDHR).

- 72-hour LOOP with second line of protection (Scram and ECC) is assessed against the criteria for plant state DBC-4, for scram conservatively as no DNB (assessed as part of the CLOF study), and for ECC the LOCA criteria of limits on clad temperature and clad oxidation. The containment aspects (following ECC) are bounded by that in the LBLOCA and MSLB analysis, see section 15.5.3.4 and 15.5.3.7.

Sequences involving the preventive measure of trip to house load, and sequences with failure of scram, which use ASF instead, and have not yet been assessed.

For the infrequent 168-hour LOOP, refill of LUHS tanks and standby AC diesel tanks from onsite or mobile sources is claimed. The required power would be provided by the alternate AC. To support the 168 hour LOOP case, operator action will be required to refill LUHS tanks after 120 hours with three LUHS trains available, or after 72 hours with two LUHS trains available.

RELAP5-3D is used to model the plant response. Note that only the long-term (DHR-related) aspects are discussed here; the short term (scram aspects) are part of the CLOF study.

Plant parameters are conservative. A starting reactor power of 102 % is used, and bounding assumptions are made for the local power of the peak pin. Conservative assumptions are used for RCP coast down curve and rod-insertion profile. Reactivity coefficients are also conservative. For Scram, a single stuck rod is assumed. The most limiting RPS and DPS trips are modelled on the assumption of a single failure.

The PDHR assessment confirms that with minimum safety system availability no sustained voidage occurs in the upper plenum demonstrating that fuel cooling is maintained.

The ECC assessment confirms that there is a significant margin to the PCT limit of 1204 °C throughout the transient. The core remains covered during the transient so no clad oxidation occurs.

The Reactor Circuit pressure remains below the design pressure and the pressuriser safety valves do not lift. As part of the PDHR sequences, ASD is effective at maintaining SG pressure below the main steam system design pressure throughout the transient. Assessment of radiological release is ongoing.

As part of the ECC sequences, the pressuriser safety valves predict lift prior to the initiation of ECC, and the SGRVs are effective at maintaining SG pressure below the main steam system design pressure. Demonstration that containment remains intact in the ECC sequences is bounded by the assessment of MSLB or LBLOCA in section 15.5.3.4 and 15.5.3.7. Assessment of radiological consequences outside of containment is ongoing.

Sensitivity studies have been carried out (as reported in the Analysis Summary [23]) modelling other loss of flow faults, which results in a similar fault progression. Furthermore, sensitivity studies were carried out to determine the most limiting trip parameters. Scram on the basis of losing power to the CRDMs was also modelled as a sensitivity study.

15.5.3.7 Analysis of Core Cooling for Loss of Coolant Accidents

This grouping considers the following PIEs:

- LOC.1.1.01: Small un-isolable LOCA
- LOC.1.2.01: Small isolable LOCA
- LOC.2.1.01: Intermediate un-isolable LOCA
- LOC.2.1.03: LOCA due to spurious reactor circuit relief valve lift
- LOC.2.1.04: LOCA due to spurious primary blowdown
- LOC.2.1.05: CRDM LOCA (LOCA aspects only; noting that the reactivity aspects will be covered in section 15.5.3.1 above in a future version of this chapter)
- LOC.2.2.01: Intermediate isolable LOCA
- LOC.2.2.03: LOCA due to spurious opening of CSCS
- LOC.3.1.01: Large Un-Isolable LOCA.

Analysis has so far been carried out for the bounding faults of LBLOCA and unisolable Intermediate Break Loss of Coolant Accident (IBLOCA), and for the other faults is still ongoing and will be reported in the next update of this chapter (Version 3 of the E3S case).

LOC.3.1.01: The most bounding case is considered to be a double guillotine failure of a cold leg pipe for assessment of fuel limits and that of a hot leg break for assessment of containment pressure limit. The coolant will escape from the break site causing a rapid depressurisation of the RCS limited by the break size. The rapid pressure loss causes coolant to flash to steam within the RCS further reducing the available coolant. Without adequate coolant this leads to fuel and clad overheating, fuel melt, and radiological release.

LOC.2.1.01: An IBLOCA is defined as being beyond the make-up capacity of the HPIS o CVCS. The coolant will escape from the break site causing a depressurisation of the RCS limited by the break size. The exact fault progression depends on the location of the leak size. Without adequate coolant this leads to fuel and clad overheating, fuel melt, and radiological release.

The following sequences have been analysed with the following success criteria:

- Both LBLOCA and IBLOCA with Scram and ECC are assessed against the criteria for plant state DBC-4 (noting that the LBLOCA IEF suggests that it could be assessed as a DEC-A fault, but conservatively and in line with RGP it is assessed DBC-4), meaning limits on clad temperature and clad oxidation. The containment pressure (for the leak plus ECC) is also assessed for LBLOCA.

RELAP5-3D is used to model the plant response. GOTHIC is used to model the containment conditions.

Plant parameters are conservative. A starting reactor power of 102 % is used, and bounding assumptions are made for the local power of the peak pin. Conservative assumptions are used rod-insertion profile.

For Scram, a single stuck rod is assumed. The most limiting RPS and DPS trips are modelled on the assumption of a single failure. Note that for IBLOCA the trip parameters take account for the different plant behaviour for different leak locations. No operator actions are required. Rationale for the selection of trips is provided in the Analysis Summary report [23].

The analysis demonstrates that the Scram and ECC safety measures are effective at protecting the plant for a LB LOCA assessed using bounding initial conditions and assumptions, pending the outstanding issues for Scram and ECC that are discussed in the performance analysis report [23].

The bounding LB LOCA case was found to be a double guillotine failure of Cold Leg 1, with two accumulators unavailable. The transient has a good margin to the PCT limit and a large margin to the clad oxide limit. This demonstrates that Scram and ECC are able to control the fuel temperatures to within safety limits even under the most severe LB LOCAs.

The assessment against containment limits is discussed in section 15.5.3.10 below. Containment remains intact; the assessment of radiological consequences outside of containment is still ongoing.

Sensitivity studies have been carried out (as discussed in the Analysis Summary report [23]) modelling differing break locations and discharge coefficients – it was observed that the largest breaks may not have the most severe consequences. Furthermore, sensitivity studies were carried out to determine the most limiting trip parameters. Sensitivity studies were also carried out with RCPs running and coasting down, given that they are not qualified for the resulting steam conditions in containment.

15.5.3.8 Analysis of Primary Circuit to Secondary Circuit Leakage

This grouping considers the following PIEs:

- LOC.2.1.02: LOCA due to SG tube rupture (SGTR)
- LOC.2.2.02: LOCA due to CSCS Tube Rupture (in shutdown modes only).

Analysis has so far been carried out for SGTR, and for CSCS tube rupture fault is ongoing and will be reported in a future update of this chapter.

Three cases are presented:

1. Case 1 – Demonstrates acceptance criteria compliance for the PDHR response to an SGTR for CoFT, secondary circuit pressure limit and SG overfilling.
2. Case 2 – Demonstrates that if Scram fails ASF can control reactivity through adequate boron injection and mixing.
3. Case 3 – Demonstrates CoFT and SG overfilling acceptance criteria are met for SGTR and LOOP for PDHR. Coincidental LOOP upon SGTR fault initiation causes the pressuriser heaters, CVCS, main feedwater systems, and RCPs to be ‘automatically isolated’ as their power source would not be available.

For the PDHR and LOOP cases, the acceptance criteria compliance is demonstrated. The ASF case demonstrates that in the event of a single tube SGTR and Scram failure, the CoR safety methods are adequate for shutting and holding down the reactor.

While the ASF method of CoR is suitable for shutting down the reactor should Scram be unavailable during an SGTR, there is no automatic leak termination once ASF is initiated due to the requirement to provide high pressure borated water to the RCS. Therefore, safe depressurisation of the plant, managing reactivity control, whilst minimising leakage and steam release will require further work to optimise the plant response.

For all cases, the PDHR functionality while running with 2oo3 trains is successful in providing sufficient cooling for the plant in post-Scram conditions.

The SGTR results presented in by this assessment provide confidence that the overall plant response to a SG tube rupture can be optimised to meet all relevant acceptance criteria.

15.5.3.9 Analysis of Pressurized Thermal Shocks

This analysis is ongoing and will be reported in a future update of this chapter.

15.5.3.10 Analysis of Pressure–Temperature Transients in the Containment

The following scenarios need to be analysed as bounding cases:

- LOC.3.1.01: Large un-isolable LOCA
- ICF.3.2.03: Excessive Steam Demand due to Large Unisolable Steam Leak (also known as **Unisolable MSLB**)

These cases involve not just the steam pressure from ECC initiation but also that arising from a primary or secondary leak, respectively, and therefore bound all other faults.

Both are assessed against DBC-4 criteria, meaning that containment remains intact.

RELAP5-3D is used to model the plant response and GOTHIC is used to model the containment pressure.

Plant parameters are conservative. A starting reactor power of 102 % is used.

MSLB: The results of the containment thermal analysis show that the maximum pressure predicted for the initial pressure peak during the MSLB blowdown occurs with a good margin to the acceptance criterion. The maximum pressure predicted for the pressure peak occurring during and following ASD is higher but still provides a margin to the acceptance criterion.

LBLOCA: The maximum containment pressure predicted during the initial RCS blowdown shows a small margin to the acceptance criterion, even if the lowest free-air volume is used (when considering all design options under consideration). The maximum pressure predicted at the point of rollover shows a good margin to the acceptance criterion.

15.5.3.11 Analysis of Radiological Consequences during Bounding Anticipated Operational Occurrences and Design Basis Accidents

The methodology for conducting design basis radiological consequences assessment is presented in [48].

The methodology identifies LB LOCA and SGTR as bounding fault groups for initial assessment of onsite and offsite radiological consequences. Limitation of the available input information are addressed via simplifications in the assessment methodology, based on RGP and conservative assumptions. As the design develops and input information matures, the methodology will be updated to reduce the conservatism and uncertainty in the assessment.

Any assessment of radiological consequences carried out will be used to provide a comparison against the RR SMR project targets in Version 3 of the E3S case.

15.5.4 Analysis of Design Extension Conditions without Significant Fuel Degradation

15.5.4.1 DBC-4 Analyses in Lieu of DEC-A

In line with UK RGP, the Rolls-Royce SMR E3S design principles [5] define a wider range of sequences as DBC-4 when compared to wider international practice. Therefore, analysis for some low frequency sequences that are below the frequency cut off for design-basis analysis has been completed using design-basis methodology, even though such sequences and events are typically defined as DEC-A by the IAEA.

The following sequences (starting from the list of design-basis faults in section 15.5.3 above) have been assessed as part of the design basis assessments as DBC-4:

- Frequent faults and failure of first protective safety measures
- Station Black Out (SBO)
- Complete Loss of Feedwater to the SGs
- Loss of cooling to the SFP
- Loss of Ultimate Heat Sink
- Large Break LOCA.

15.5.4.2 DEC-A Analyses that are Carried out on a Best-Estimate Basis

The following DEC-A analyses will be carried out on a best-estimate basis:

- Aircraft impact
- Analysis of a category C ECC variant that is intended for use in SBO (LOC.1.0.02 – LOOP for 168 hours).

These analyses are ongoing and will be reported in Version 3 of the E3S case.

15.5.5 Analysis of Design Extension Conditions with Core Melt

This section presents the DEC-B analysis under the following heading structure:

- 15.5.5.1 General Approach to Design Extension Condition-B
- 15.5.5.2 Potential Severe Accident Phenomena Progression without mitigation
- 15.5.5.3 Key Severe Accident Phenomena Considered Within the Design
- 15.5.5.4 Containment Safety Measure [JM01] (variant 4) for Design Extension Condition-B
- 15.5.5.5 Description of the Containment Safety Measure [JM01] subfunctions
- 15.5.5.6 DEC-B deterministic analysis
- 15.5.5.7 Generation of Source Term
- 15.5.5.8 Analysis of radiological consequences of design extension conditions with core melting
- 15.5.5.9 Demonstration of Practical Elimination.

15.5.5.1 General Approach to Design Extension Condition-B

The Beyond Design Basis (BDB) deterministic DEC-B safety analysis will demonstrate that the safety criteria are met with a high confidence level for scenarios involving fuel melt. The methodology [50] can be defined as a set of procedures and guidance for the analysis studies to be carried in a manner that ensures best estimate results. The methodology uses calculation code(s) which are supported by VVUQ demonstrating they are appropriate for their modelling applications.

The aim of this chapter is to provide the evidence to underpin the claims and arguments made within the E3S case, as identified within Appendix A (section 15.11).

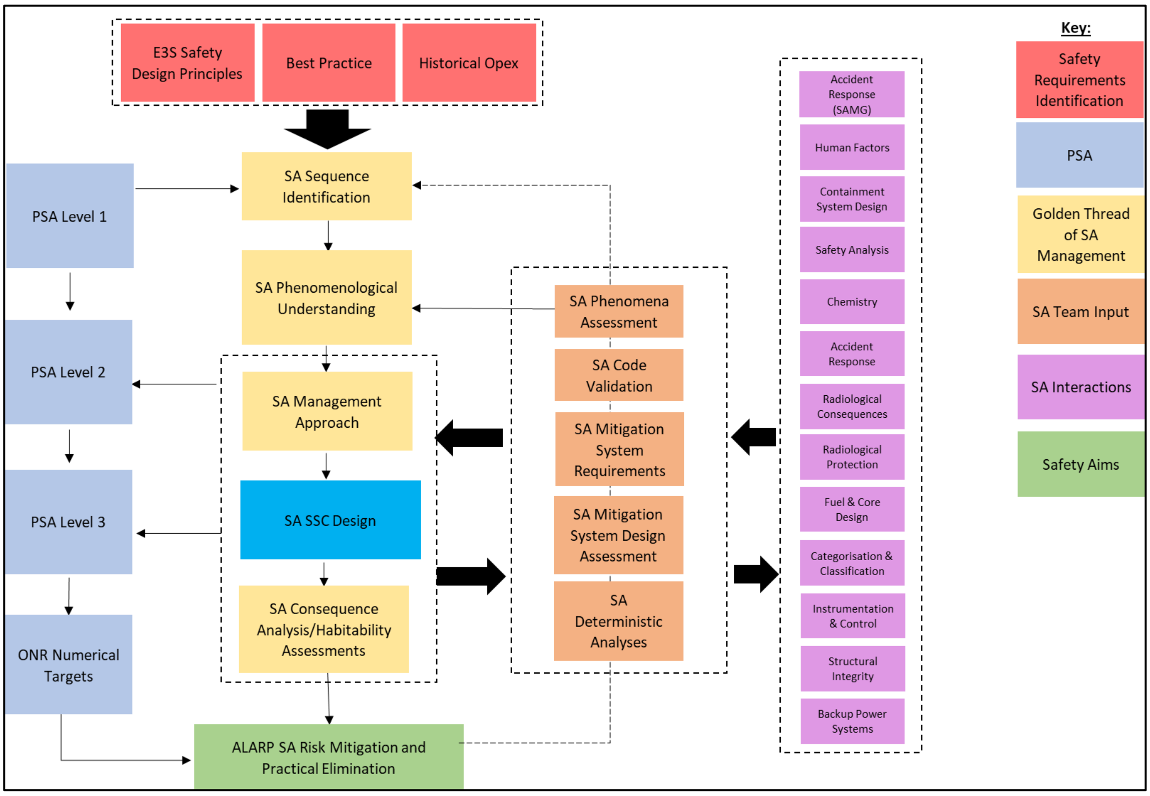


Figure 15.5-1: RR SMR Severe accident strategy.

15.5.5.1.1 RR SMR Severe Accident Management Strategy

The severe accident management strategy describes the process that provides demonstration that for postulated accidents involving fuel melt, phenomena associated with core melt are either prevented or mitigated where reasonably practicable to ensure that risks are ALARP by level 4 DiD design provision. The process for providing this evidence allows for demonstration that the design provision reduces risks to ALARP and the practical elimination of Large or Early releases.

Figure 15.5-1 illustrates the golden thread of severe accident management, the gold sequence is in the centre of the diagram. The light blue sequence concerns PSA; the orange, SAA; the dark blue, severe accident SSC design; the purple, interfaces; and red, requirements.

There are iterative aspects of the strategy centred around the design of severe accident mitigative measures (which are part of variant four of the CSM [JM01]) taking into account the results of SAA (positioning and sizing of SSCs and timings to allow for operator action) and PSA. If practical elimination targets are not met for event sequences, design provision will be reviewed to ensure that risks are ALARP.

15.5.5.1.2 Severe Accident Sequence Identification

The first step in severe accident management is the identification of severe accident fault sequences. Such fault sequences are associated with severe accident scenarios that can cause the failure or bypass of the final confinement barrier, the containment structure.

Severe accident sequences are identified based on:

- A review of RGP – This may provide an initial matrix of plant conditions, severe accident phenomenology etc.
- Historical operator experience.
- Safety requirements, taken from the E3S design principles [5], provide established and endorsed international practices for reactor and plant design and operation, providing a design framework by which the design is evaluated and developed.
- The results of the Level 1 PSA, together with engineering judgement, are used to produce an appropriate and representative set of Plant Damage States (PDSs).

15.5.5.1.3 Severe Accident Phenomenological Understanding

After a review of the identified severe accident sequences and potential accident progression, the phenomena of most relevance are identified and grouped. A Phenomena Identification and Ranking Table (PIRT) is used to provide a general understanding of the phenomena, ranking them according to their impact on the severe accident progression, and identifying the main conditions (or combinations of situational characteristics) where individual phenomena are likely to cause significant threats. A summary of the PIRT is reported in [51].

The phenomenological understanding is used to select a list of representative and suitably bounding accident sequences for the SAA of DEC-B. These sequences should demonstrate the range of phenomena expected for the RR SMR and provide limiting examples of these phenomena to substantiate safety claims.

The final list of bounding accident sequences, following DRP3, will be derived after the probabilistic and deterministic screening step covering all relevant modes of operation. The sequence selection process is described in [50]. It should be noted that at RD6, which the current SAA is based on, reasonably bounding sequence selection is based on engineering judgement and RGP, for full power modes only.

15.5.5.1.4 Severe Accident management approach/strategy

Once an understanding of severe accident phenomena and progression is gained the next stage in the process involves defining the severe accident management approach/strategy. This is concerned with deriving strategies to cope with the phenomena that threaten integrity of the Containment System [JMA], which will act as a physical barrier to confine radioactive material during a severe accident.

The holistic severe accident management approach is executed through variant four of the CSM [JM01], the severe accident management strategy is discussed within [52]. Severe accident SSC functional requirements are identified for CSM [JM01] subfunctions, these are the specific purpose or objective that must be accomplished to achieve their duty. These are derived based on the defined strategy and RGP, including lessons learnt from previous nuclear accidents.

15.5.5.1.5 Severe Accident Structures Systems and Component design

Severe accident SSCs (as part of CSM [JM01]) are designed based on the severe accident management strategy and functional requirements defined in the RR SMR requirements management database. Non-functional requirements (e.g. flow rates etc.) are also identified during the design process, these form part of the success criteria. During design, requirements are placed on: categorisation and classification, instrumentation and control, structural integrity, civil engineering, electrical engineering, human factors and equipment qualification.

Requirements are entered into modules within the RR SMR requirements management database which are linked to the appropriate SSCs.

The design information representing Level 4 DiD SSCs is included within the MAAP model to enable SAA to be performed on the selected accident sequences. Analysis is then performed to determine or confirm the capacity of equipment and time allowance for operator action which will then feed back into the design process. The design process is iterative, as discussed in Section 15.5.5.4.2.Severe Accident Analysis

SAA evaluates the performance of the severe accident SSCs, thereby showing that the SSCs are effective in preventing or mitigating the identified phenomena and where the limits of their effectiveness are.

SAA is used:

- To show the absence of cliff-edge effects or to determine the margin to a cliff-edge effect, to support the justification of the DiD provisions in the design.
- To perform sensitivity studies on key parameters, analysis assumptions, and the timing of actions.
- Provide justification, or otherwise, of any further preventative or mitigative measures beyond those derived from engineering analysis, Design Basis Analysis (DBA) and PSA.
- During this process requirements on; equipment qualification, C&I, electrical engineering, structural integrity, human factors (operator action and human accessibility), and civil engineering are refined.
- Any shortfalls or improvements in the design may be revealed, this provides feedback to the SSC design.

Analysis of DEC-B is performed for three reasonably[3] bounding examples of the most limiting fault categories expected for the RR SMR at RD6. Following DRP3, analysis of DEC-B will include a more complete set of bounding accident sequences.

15.5.5.1.6 Severe Accident Consequence Analysis/Habitability Assessments

Severe accident source analysis considers possible release paths and the physical/chemical behaviour of fission products [48]. This source term analysis allows for severe accident consequence analysis to be performed.

Severe accident source term analysis will be performed following DRP3 (using DRP1 and DRP2 design information) using the results of the SAA to determine the possible consequences under severe accident conditions for DEC-B as part of the severe accident deterministic case and Level 2 PSA, and for beyond DEC-B as part of the Level 3 PSA.

[3] At RD6 reasonably bounding sequence selection is based on judgement and the capability within the MAAP model in line with the process described within Section 15.5.5.6 excluding results of the Level 1 PSA as this was unavailable, for full power modes only.

Habitability assessments will be carried out following DRP3 (using DRP1 and DRP2 design information) using source term information for relevant control locations and areas identified as requiring local operation actions in the event of a severe accident.

15.5.5.1.7 As Low As Reasonably Practicable Severe Accident Risk Mitigation and Practical Elimination

The SAA forms part of the evidence to justify claims and arguments that specific severe accident phenomena are prevented by design or, where they cannot be prevented, that the design measures mitigate the accident progression and radiological consequences of severe accidents.

Accident sequences that may lead to an early or large radioactive release will be assessed against practical elimination targets. The results of the PSA (including probabilistic representation of severe accident scenarios) provide context for ALARP judgements.

15.5.5.1.8 Interface with Probabilistic Safety Assessment

Inputs to SAA from PSA include the results of the Level 1 PSA, which, with engineering judgement, contribute to the development of PDSs and following on from this, selection of bounding sequences following DRP3 for the SAA of DEC-B and Level 2 PSA.

The outputs from the SAA to PSA include:

- Severe accident phenomena and progression analysis.
- A basis for estimating radiological releases (magnitude, timing and characteristics) for representative end points in the Level 2 PSA.

15.5.5.1.9 Other Outputs from Severe Accident Analysis

SAA is used to support the future development of Severe Accident Management Guidelines (SAMG), and procedures considering the adverse working environments that could be encountered during and following a severe accident.

15.5.5.1.10Assessment of Design Extension Condition-B design provision

The RD6 assessment of DEC-B design provision utilises a limited set of reasonably bounding severe accident sequences from the most limiting fault categories expected for the RR SMR, these are presented in Table 15.5-1. This demonstrates that the CSM [JM01] SSCs are able to achieve a Severe Accident Safe State (as described in [5]) where reasonably practicable to ensure that risks are ALARP. Following DRP2 (RD8 design maturity gate) this analysis will be expanded to cover the full range of fault categories and operational modes expected for the RR SMR, with sequences selected based on the output of a mature Level 1 PSA.

Table 15.5-1: RD6 SAA List

Accident Sequences at RD6	Sequences Description	Accident Sequence Base Cases
LBLOCA	A double ended guillotine failure of the cold leg with failure of all duty heat removal systems	LBLOCA occurs during Plant Operating State (POS) Mode 1 or 2. Duty make-up systems fail, CDHR [JN03] and PDHR [JN02] fails. ECC [JN01] Phase 1 successfully operates with one accumulator. ECC [JN01] phases 2 and 3 fail. Core melt conditions are reached. Reactor Vessel Cavity Injection System (RVCIS) [JNM], Passive Containment Cooling (PCC)/LUHS [JNK] and Passive Autocatalytic Recombiners (PARs) are successful.
Slow Depressurisation	A breach within the RCS [JE] with a breach size of 25 mm occurring in the cold leg pipework near the RPV nozzle.	A 25 mm LOCA (break size selected on the highest hydrogen production of the pre-analysis test cases) occurs during POS Mode 1 or 2. Duty make-up systems fail, CDHR [JN03] and PDHR [JN02] fails. ECC [JN01] Phase 1 successfully operates with one accumulator and Automatic Depressurisation System (ADS). ECC [JN01] phases 2 and 3 fail. Core melt conditions are reached. RVCIS [JNM], PCC/LUHS [JNK] and PARs are successful.
SBO	Loss of all AC electrical systems, resulting in the loss of the main coolant pumps and heat removal systems.	SBO occurs during POS Mode 1 or 2. Duty make-up systems fail, CDHR [JN03] and PDHR [JN02] fails. ECC [JN01] Phase 1 successfully operates with one accumulator and ADS[3]. ECC [JN01] phases 2 and 3 fail. Core melt conditions are reached. RVCIS [JNM], PCC/LUHS [JNK] and PARs are successful as no electrical power is required.

Further detail of the accident sequences summarised within Table 15.5-1 and associated sensitivity studies is provided within Section 3 of [18].

15.5.5.2 Potential Severe Accident Phenomena Progression without mitigation

This section provides a description of the physical and chemical processes and phenomena, in-vessel and ex-vessel, that might occur during the progression of a severe accident, without any severe accident SSCs/mitigative measures in place to prevent/mitigate phenomena.

Physicochemical phenomena associated with severe accident progression behaviours are well documented (e.g. [36], [53] and [54]). Different phenomena can occur at various stages of a postulated severe accident and are the result of the various physical, thermodynamic, and chemical processes related to fuel degradation and the interactions between molten fuel and the various materials it may come into contact with.

Severe accidents often take the form of complex accident progression sequences spanning across several phases. The specifics of such sequences are difficult to summarise due to the number of factors involved which may affect the accident's progression, such as: timings of fuel melt and relocation, temperature distribution and coolant flow patterns, or quantities and concentrations of hydrogen generated. However, the physical processes and their order of occurrence are much more consistent and may be discussed using a generic sequence. A general sequence of severe accident progression is shown in the diagram below.

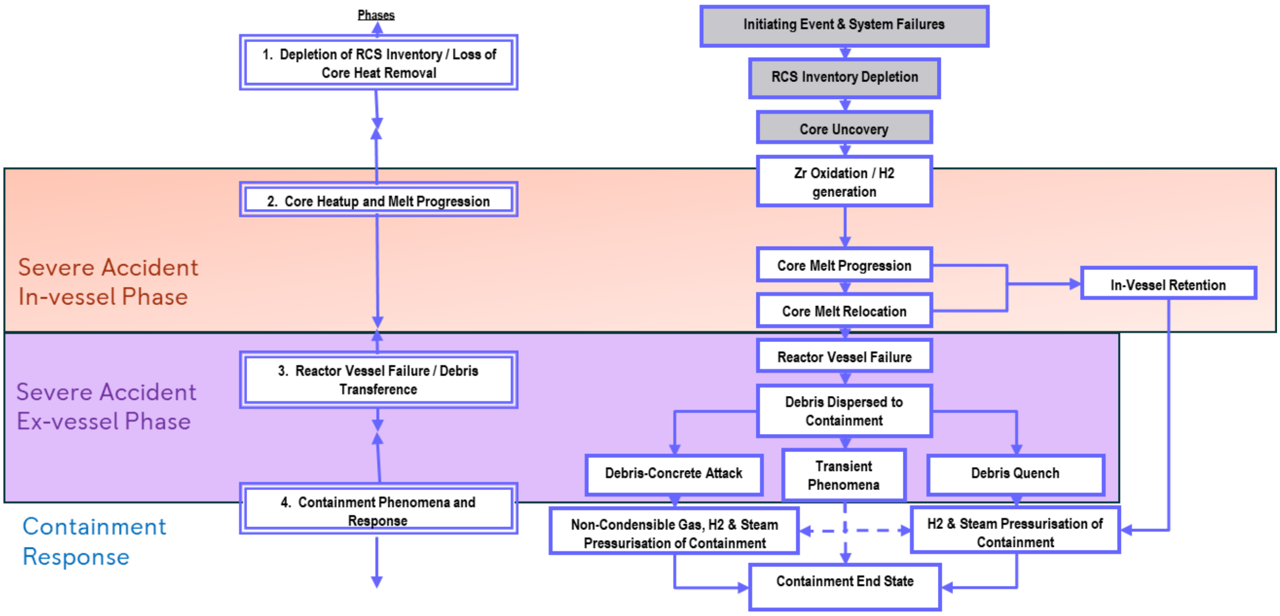


Figure 15.5-2: Simplified Accident Progression Paths for PWR at Power

15.5.5.2.1 Pre-cursor Phase

This phase covers the depletion of the RCS [JE] inventory and/or loss of core heat removal. A PIE and/or a combination of duty system failures can lead to the core becoming uncovered. If failures of specific safety systems and other fault condition safety features designed to recover from such events also occur, the plant may progress to a severe accident condition.

Fuel damage may occur prior to core melt due to DNB in a Design Basis Fault, the potential impact of DNB occurring prior to phase 2 is expected to have little impact on severe accident progression. Potential DNB excursions are considered within the design-basis analysis.

15.5.5.2.2 In-Vessel Phase

The in-vessel phase begins as the core uncovers, exposing the fuel cladding to high temperature steam, resulting in clad oxidation. The oxidation of Zirconium in steam is a highly exothermic process which produces hydrogen and releases significant quantities of heat. Following this, and in the absence of water injection, the core will begin to melt. The centre of the core is generally first to melt due to the power distribution of the reactor during normal operation and due to its limited heat transfer to the vessel wall. As the cladding and fuel pellets begin to melt this inhibits their ability to retain fission products, and consequently these are released around the core.

The melt progresses downwards, damaging the steel support structures which maintain the fuel's geometry. The molten corium will eventually end up forming a pool within the vessel lower head, this pool is built up in distinct layers owing to the different densities and melting points of materials within the core. The pool is in direct contact with the reactor vessel and, in the absence of the external cooling provided by IVR, begins to ablate the wall material.

15.5.5.2.3 Ex-Vessel Phase

For potential severe accident phenomena progression without mitigation, following a period of ablation, the vessel wall fails. If the vessel is depressurised relative to the containment, then the molten corium flows out into the vessel cavity. If the vessel is still held at pressure, there is potential for the molten corium to be forcefully ejected into containment, resulting in phenomena such as High Pressure Melt Ejection (HPME) and DCH. The escape of molten corium presents significant challenges for the containment during this phase, once unconfined it is difficult to provide cooling or containment to the molten corium and several severe accident phenomena may occur.

15.5.5.2.4 Containment Response

Severe accident phenomena postulated to occur in the in-vessel and ex-vessel phases place an increased demand on the containment structure, in terms of withstanding pulsed and/or prolonged pressure and temperature transients and, where melt is discharged into the RPV cavity [UJA], chemical attack. In an unmitigated circumstance, these phenomena may result in a breach of the containment [52].

15.5.5.3 Key Severe Accident Phenomena Considered Within the Design

The RR SMR is designed to withstand severe accident phenomena. However, the following sections are included to highlight some of the key specific phenomena that could occur if an event is not mitigated.

15.5.5.3.1 High Pressure Melt Ejection (HPME) and Direct Containment Heating (DCH)

Within certain severe accident sequences the rapid accident progression may result in increased pressure within the RCS. If the RCS is not depressurised, this may result in a vessel failure while there is a significant pressure differential to the containment atmosphere. The relatively high pressure in the vessel and primary coolant system may result in the ejection of molten corium into the containment, this phenomenon is known as HPME [53] [55].

Upon failure of the vessel molten corium is forcefully ejected throughout containment as entrained particulate along with any remaining steam and remaining water inventory in the RPV. The ejection of aerosolised corium into containment may contribute to the breach of acceptance criteria through the following mechanisms [55]:

- Creating excess pressure and temperature in containment atmosphere increasing the risk of containment failure, this can be described as DCH.

- Directly damaging the containment vessel, reducing its efficacy as a barrier against the release of radioactive material.

- Creating a source term for radioactive aerosols to release to the environment if the containment should fail.

- Generating additional hydrogen within containment due to the corium’s high temperature and relatively large contact area with steam.

DCH may occur through two pathways; the debris heating up the atmosphere surrounding it as it cools, or oxidation of the debris, this may be exothermic, creating additional heat as well as producing hydrogen from its interaction with steam [56].

HPME and DCH is prevented within the RR SMR design for DEC-B through incorporation of the Severe Accident Depressurisation (SAD) and IVR functions of the CSM [57]. SAA is used to demonstrate that for DEC-B, SAD and IVR are successful in preventing HPME and DCH.

15.5.5.3.2 Hydrogen Combustion

In a PWR during severe accident conditions, hydrogen combustion presents a major challenge to the management of accidents and the prevention of release. High concentrations of hydrogen within the containment may combust, deflagrate or detonate creating high pressure conditions which may compromise the containment. The most common mechanism of hydrogen production is the oxidation of zirconium cladding by steam to produce zirconium oxide, hydrogen and heat. The reaction occurs during high temperature conditions and the rate of oxidation accelerates with increased temperature, meaning that as the reaction progresses the heat it generates creates a positive feedback loop [58].

During fuel melt conditions within the RPV there is a relatively large mass of zirconium exposed to the high temperature steam, hydrogen produced will be transferred to containment during depressurisation of the RCS, either intentionally through depressurisation of the RPV or via a break in the RCS. The largest quantity of hydrogen expected for the RR SMR is likely to occur during extended periods of fuel / cladding-coolant interaction [58].

Hydrogen is also produced from hydrolysis and the oxidation of other steel components forming the RPV internals and core barrel etc. Generally, these processes evolve over longer timescales compared to the hydrogen production from fuel clad oxidation. Further sources of hydrogen may come from ex-vessel mechanisms such as HPME or MCCI, if these are predicted to occur.

The Hydrogen Reduction System (HRS) function of the CSM [57] is designed to maintain hydrogen concentrations in containment within design conditions during a postulated DEC-B to ensure that the containment remains intact. The HRS is designed to remove the hydrogen produced from 100 % fuel clad oxidation. The containment is also of an open design with a large free air volume which aids mixing to prevent localised hydrogen build up.

Detonation of combustible gas is prevented for DEC-B within the RR SMR design through incorporation of the HRS (i.e. in-vessel hydrogen sources only). Ex-vessel sources of hydrogen, such as HPME or MCCI are prevented by; the SAD function, IVR function and Containment Cooling and Spray Function (CCSF) of CSM [57]. SAA is used to determine the effectiveness of the removal of hydrogen from containment in DEC-B.

The steam concentration within containment maybe reduced, enhancing the flammability of the containment atmosphere by some severe accident mitigative measures such as sprays [59].

15.5.5.3.3 Steam Explosion

Steam explosions are a phenomenon resulting from the rapid transition of water from liquid to vapour. This occurs upon contact with surfaces that are at significantly higher temperatures than water’s boiling point. The water begins to boil rapidly leading to a rapid expansion. The continued expansion generates a pressure wave which contains sufficient energy to move or deform nearby structures, i.e. an explosion. In Light Water Reactors (LWRs), steam explosions may occur inside the RPV (in-vessel) or outside the RPV (ex-vessel).

In-vessel steam explosions may occur during core melt scenarios where the debris relocation into the (still flooded) lower head results in the rapid vaporisation of the remaining vessel inventory, resulting in a pressure which increases more rapidly than pressure relief systems can vent. These steam explosions may challenge the containment of the RPV resulting in ex-vessel phenomena such as HPME, MCCI, or ex-vessel steam explosions [53]. However, international research demonstrates that the likelihood of in-vessel steam explosions challenging the containment of the RPV is unlikely [60] [61].

For unmitigated severe accident sequences, a breach of the RPV will result in a relocation of molten corium into the reactor cavity. If molten core debris is ejected into a flooded RPV Cavity [UJA] following vessel failure the interaction between the molten corium and the flooded cavity rapidly generates steam within containment, potentially leading to a steam explosion. Such an event presents a significant challenge to containment and may provide a source term for an energetic release [62].

Ex-vessel steam explosions are prevented within the RR SMR design for DEC-B through incorporation of the CSM [57]. SAA is used to demonstrate the effectiveness of CSM in maintaining DEC-B [57].

15.5.5.3.4 Containment Overpressure

Containment overpressure is a potential failure mode during severe accident scenarios. Pressure rises are likely to be most significant following a break in the RCS due to the release of steam and hydrogen directly into containment. Additional source of pressure may be generated through MCCI.

Under some circumstances, a steam explosion, hydrogen deflagration or hydrogen detonation may produce a pressure wave, which might threaten containment integrity.

Containment overpressure is mitigated in DEC-B through incorporation of the CCSF subfunction of the CSM [57]. SAA of DEC-B is used to determine the effectiveness of the removal of heat and pressure from within containment.

15.5.5.3.5 Molten Corium Concrete Interaction

MCCI is an ex-vessel phenomenon where, upon failure of the lower head of the RPV, the molten corium enters the reactor cavity. Upon corium dry out, cooling is predominantly provided by the erosion of the concrete basemat. This erosion causes direct damage to the containment as well as producing non-condensable gases from the thermal decomposition of the concrete. These non-condensable gases contribute to the pressurisation of the containment atmosphere and are potentially difficult to remove [63]. Additional flammable gases such as hydrogen or carbon monoxide may be produced from the interaction of non-condensable gases with unoxidized metals from the reactor.

MCCI is prevented within the RR SMR design in DEC-B through incorporation of the CSM [57], specifically through the SAD and IVR subfunctions. SAA is used to demonstrate the effectiveness of CSM in maintaining DEC-B [57].

15.5.5.3.6 Chemistry Related Phenomena

The progression and development of severe accident phenomena within the RR SMR may be affected by chemistry related phenomena as discussed below.

Core Degradation and Relocation

The timescales and temperatures over which the degradation and subsequent relocation of the core occur depends on the chemical composition of the; fuel, cladding, control rods and coolant, as well as the thermal hydraulic conditions of the system [64].

During core degradation the ballooning of cladding increases the area of zirconium exposed to steam, resulting in increased hydrogen production.

Materials with higher melting points and differing densities may slow the melt progression and affect stratification in the lower head [64]. The light metal layer is a relatively thin layer atop the stratified core material which is made of structural materials from the core (Steel and potentially zirconium). The quantity of these materials determines the thickness of the layer, where a thinner layer creates in a greater 'focussing effect' resulting in a higher heat flux across the lower head [53].

Fission Product Transport within the RCS

Fission product release and transport are key severe accident phenomena and are important for determining source terms. The fission products contained within the core are dependent on the composition, burnup, and history of the fuel. The fuel temperature during the accident influences the rate and type of fission product release from the core, during core heat-up and melting, volatile fission products such as; caesium, iodine and noble gases are released more readily. The vaporised fission products are transported away from the core into the cooler regions of the RCS where they may aerosolise and deposit on the primary circuit pipework, the transport of these fission products reduces the decay heat within the core, increasing the temperature of the RCS which if left unmitigated, could lead to localised RCS failure [54] [53].

Incorporation of the SAD and IVR functions of the CSM [57] within the RR SMR design for DEC-B prevent RCS failure.

Fission Product Release to Containment

Depending on the type of fault, the release of fission products to containment may follow two different pathways: during ICFs fission products may be released through the RCS depressurisation systems, and for open circuit faults they may be released through breaks in the primary circuit.

Fission Product Behaviour in Containment (Iodine)

A large fraction of the core inventory of iodine could eventually reach the containment during a severe accident. The dominant forms of iodine released into containment will be aerosols and gaseous metal iodides. Aerosolised iodine is expected to deposit on in-containment surfaces.

Iodine may be retained within water pools within containment (such as in the containment sump), as either iodide, I^-, or molecular iodine, I_2. The molecular iodine undergoes hydrolysis, which depends on the temperature, pH, and concentrations of iodine species. As such the pH within water pools is important in determining the rate of iodine capture from the containment atmosphere. The detailed mechanism for the capture of iodine in containment water is described in [65].

Other Chemistry Related Phenomena

Other phenomena which may affect the progression and development of severe accident phenomena within the RR SMR include:

- Oxidation of the RPV
- The chemical composition of the cooling water, this can affect the coolability of the lower head.

15.5.5.4 Containment Safety Measure [JM01] (variant 4) for Design Extension Condition-B

15.5.5.4.1 Description of the Containment Safety Measure [JM01] (variant 4)

The CSM [JM01] has been incorporated into the RR SMR design based on the understanding of severe accident progression and phenomena, as described in Section 15.5.5.3. The objective of CSM [JM01] is to avoid the unplanned release of radioactive material from the RCS [JE] and the Reactor System [JA]. CSM [JM01] allocates requirements to sub-functions to achieve the confinement of radioactive material fundamental safety function.

The Containment System [JMA] (containment vessel, penetrations, equipment hatches and airlocks) forms a leak tight pressure boundary around the RCS [JE]. The Containment System [JMA] is considered the final barrier to confine radioactive material, after the fuel pellet, the fuel cladding tubes, and the pressure boundary of the RCS [JE], refer to Chapter 6 for details [12].

A holistic approach to managing severe accident progression and phenomena is taken within the RR SMR design, the strategy for severe accident management is discussed within [52]. A comprehensive fault and hazard analysis is used to identify CSM [JM01] sub-functions (severe accident SSCs) for DEC-B as discussed within [57]. Several sub-functions have been identified, as presented within Section 15.5.5.5, which are required to protect the integrity of the Containment System [JMA], or control conditions inside containment during DEC-B.

The overall aims of the severe accident management strategy are to demonstrate; that the RR SMR severe accident design provision reduces risks to ALARP, and the practical elimination of Large releases and Early large releases with a high degree of confidence.

CSM [JM01] sub-functions prevent or mitigate phenomena identified during DEC-B, as presented within Figure 15.5-3, as follows:

- Hydrogen Management – to prevent/practically eliminate containment failure initiated by a hydrogen combustion.
- Containment Heat Removal and Depressurisation – to protect the integrity of the containment, if core melt cannot be avoided, by mitigating temperature and pressure transient inside the containment.
- RCS [JE] SAD – to prevent/practically eliminate DCH to protect containment integrity. This also protects against HPME which will cause MCCI and over-pressure of containment.
- IVR – to prevent/practically eliminate failure of the RPV [JAA] to retain corium. This protects against subsequent ex-vessel severe accident phenomena e.g., HPME, ex-vessel steam explosion, MCCI.

- Depressurise Containment – to protect the integrity of the containment, if core melt cannot be avoided, by mitigating temperature and pressure transient inside the containment.

A description of these sub-functions can be found in E3S Case Tier 1 Chapter 6. Further details about the design, operation and expected performance of CSM [JM01] can be found in [57].

Phenomena deemed to be physically impossible or extremely unlikely to occur with a high degree of confidence as a result of DEC-B design provision (i.e. HPME, MCCI, ex-vessel steam explosions) are not considered. Design provisions that reduce risks to ALARP during conditions which exceed DEC-B may be considered at a later date during the Design Review (DR) process.

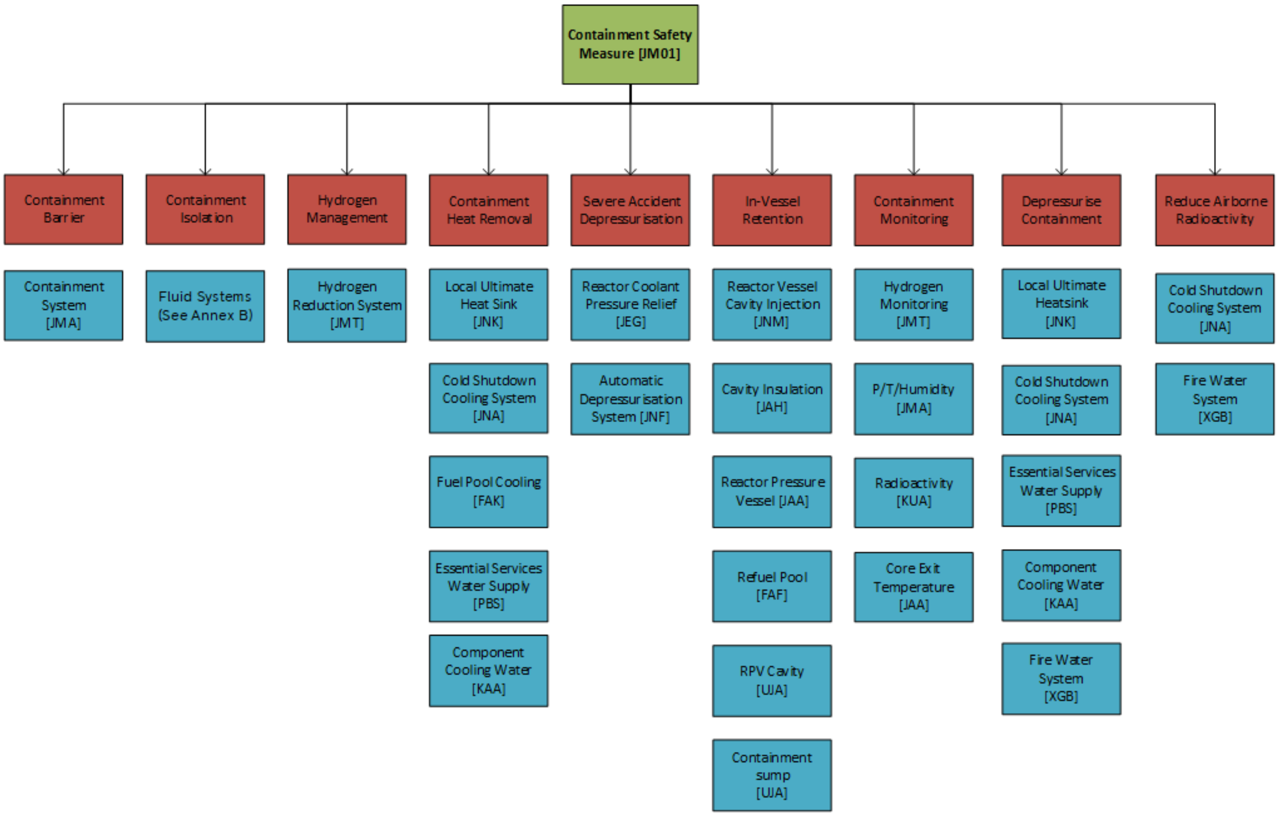


Figure 15.5-3: CSM [JM01] Variant 4 Illustrative Functional Diagram – DEC-B (Red = subfunction, Blue = SSC that supports subfunction)

Table 15.5-2:Design provision incorporated into the RR SMR design to avoid/mitigate severe accident phenomena.

Severe Accident Phenomena	CSM [JM01] sub-function / severe accident SSCs
DCH/HPME	SAD
	IVR
Ex-vessel large steam explosion	IVR and SAD
Detonation of combustible gases	HMS

Severe Accident Phenomena	CSM [JM01] sub-function / severe accident SSCs
Basemat penetration or containment bypass during MCCI.	IVR and SAD
Long term loss of containment heat removal.	Containment Heat removal
Containment Overpressure	Containment Heat removal
	Depressurise Containment

15.5.5.4.2 Design Process for Severe Accident Structures Systems and Components

This section provides the evidence to substantiate the following claim in the safety case: safety analysis informs the design of the CSM variant 4 subfunctions (severe accident mitigative systems).

Based on the severe accident management strategy, the CSM [JM01] sub-functions are assigned to protect/mitigate against specific severe accident phenomena, identified through RGP and lessons learned following nuclear accidents. Functional requirements are then derived based on this strategy. Mitigative SSCs are designed to meet functional requirements.

The design of the severe accident SSC is informed by analysis, the interaction between design optioneering and analysis is often iterative and holistic, as various design options can have a substantial impact on the model used in the analysis for individual systems and large structural components.

- The considerations for the design optioneering phase include: establishment of the severe accident mitigative SSCs necessary to deliver the functional requirements and their sizing, including; pressure and temperature limits, electrical power requirements, flow and cooling rates.

- Determining (approximately) setpoints for parameters which trigger mitigative systems, to confirm these are effective, and they allow adequate operating margins.

- Predictions of many of the characteristics of severe accident sequences necessary to support the design optioneering, for example:

    - The chronological progression of postulated accident sequences and timing of key events.

    - Changes in plant conditions (pressures, temperatures, etc) during the accident sequence.

    - The likely ‘operating envelope’ SSCs would experience and possible fluctuations in physical, chemical and radiation conditions induced by severe accident phenomena that could be outside of this ‘operating envelope’.

    - Timescales for possible accident management actions to implement or recover SSCs.

However, the representativeness of the SAA output is itself dependent on the maturity of the MAAP plant parameter file, which is described by [66]. The plant parameter file is a representation of the containment design and the design of all the systems it contains. As SSCs associated with the CSM [JM01] undergo optioneering and design (from concept to detailed design), the plant parameter file also reflects that uncertainty in system design. Therefore, the alignment of the SSC design and plant parameter file is itself an iterative process.

Furthermore, any insights gained from the sensitivity studies (supporting the design process) are then reflected in further design development. This information is then used to firm up aspects of the plant parameter file which, in turn, gives greater confidence in future sensitivity study results. This is an iterative process. Once interim (or final) design decisions are made, the plant parameter file is updated to reflect those decisions, and this updated file is used to model postulated severe accident progression in future studies.

This iterative process is performed throughout the design process to ensure that CSM [JM01] variant 4 sub-functions can deliver their functional requirements and ensure that acceptance criteria are met.

During this process, requirements on other interfacing topics such as categorisation and classification, equipment qualification, electrical engineering, C&I, human factors (operator actions), structural integrity and civil engineering are considered.

15.5.5.5 Description of the Containment Safety Measure [JM01] subfunctions

Severe accident mitigative SSCs are presented within this section at the most recent reference design point; RD7/DRP1. Due to the iterative nature of the analysis, it naturally lags the design.

Functional requirements and corresponding success criteria will continue to be developed at the next design iteration.

15.5.5.5.1 Containment of Heat Removal and Depressurisation of Containment

This section concerns both the CSM [JM01] sub-functions; containment of heat removal and depressurisation of containment.

Design information presented for the containment heat removal function is based on DRP1.

Introduction

During a postulated core melt accident (DEC-B) the Containment Heat Removal function ensures the integrity of the containment. In accident conditions heat is transferred from the molten corium inside of the RPV [JAA] to the containment atmosphere via boiling of coolant inventory in the Reactor Cavity, which leads to an increase in pressure and temperature inside containment. The Containment Heat Removal function condenses the steam, reducing the temperature and pressure of the containment atmosphere, replenishing cooling water in the Reactor Cavity. This function therefore also supports the IVR function, ensuring the retention of molten corium in the RPV [JAA], and preventing ex-vessel phenomena such as ex-vessel steam explosion and MCCI.

If unmitigated, conditions within containment may exceed acceptance criteria for pressure and the containment vessel may be breached. Failure to maintain acceptable conditions within containment may result in the loss of the containment barrier and release of radionuclides.

The CSM [JM01] can utilise two independent methods to transfer heat from inside containment to the ultimate heat sink in applicable faults. The Containment Heat Removal function prevents the Containment System [JMA] and SSC required during faults from exceeding their pressure and temperature limits. CSM [JM01] uses the following key SSC for heat removal:

- Passive Containment Heat Removal via the LUHS [JNK].
- Active Containment Heat Removal utilising the CCSF in recirculation mode, via the CSCS [JNA]/ FPCS [FAK]/Ultimate Heat Sink.

Both active and passive heat removal methods are independently capable of removing sufficient heat from containment to maintain containment pressure below design pressure.

More information on the design of the PCC/LUHS [JNK] and CCSF system, including categorisation and classification, C&I, electrical supplies and operator actions, can be found in Chapter 6 and [57], Chapter 7 [72], Chapter 8 [71] and Chapter [33].

Functional Requirements

If core melt cannot be avoided, then the integrity of the containment and RPV is protected by the containment heat removal safety function, preventing containment overpressure through containment heat removal.

The CSM [JM01] safety categorised functional requirements applicable to containment heat removal [67] are as follows:

- When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall remove heat from Containment System [JMA] to the ultimate heat sink.
- When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce the pressure inside Containment System [JMA].
- When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce the quantity of airborne radioactive material inside Containment System [JMA].

Success Criteria

The SSCs associated with containment heat removal and containment are designed to maintain the containment atmosphere within design conditions during a postulated DEC-B to ensure that the RPV [JAA] and containment remain intact.

Success criteria are presented in Table 15.3-1.

Design Process

The general design process for CSM [JM01] is described in Section 15.5.5.4.2. Parameters informed by analysis include:

- Passive Containment Cooling (PCC) Heat Exchanger Duty (per train)
- LUHS [JNK] boil-off inventory (per train)
- CCSF Peak cooling duty for a single train in recirculation mode (DEC-B)

- CCSF Maximum mass flowrate with a single train operating in recirculation mode (DEC-B)
- CCSF Peak cooling duty for a single train in spray mode (DEC-B)
- CCSF Maximum mass flowrate with a single training spray mode (DEC-B).

The pH of water pools can affect deposition and absorption rates of the iodine and iodic compounds. Further work is underway to determine the chemistry, and subsequently, the pH. This is due to provide initial results for DRP2 which will inform the decision on containment pH control. [68]

15.5.5.5.2 In-Vessel Retention (IVR)

Design information presented for the IVR function is based on DRP1.

Introduction

During a postulated core melt accident (DEC-B) the IVR function ensures the retention of molten corium in the RPV [JAA], preventing highly energetic ex-vessel phenomena such as: HPME, DCH, Ex-vessel steam explosion and MCCI.

Corium retention is achieved by cooling the RPV [JAA] sufficiently to ensure the RPV [JAA] integrity is maintained under the loads anticipated during core melt. This is achieved by flooding and cooling the reactor cavity through Reactor Vessel Cavity Injection [JNM] (RVCIS), and transferring heat from the corium, via the walls of the RPV [JAA], and coolant within the reactor cavity, to the containment atmosphere. The heat released into the containment atmosphere is removed by the containment heat removal system.

There are two phases to IVR; an initial phase which is required to flood the RPV Cavity [UJA] fully prior to core relocation, and a recirculation phase which provides coolant to the cavity to replace any coolant lost to boiling.

More information on the design of the IVR, including categorisation of the function, and classification of the measure, C&I, electrical supplies and operator actions can be found in Chapter 6 and [69], Chapter 7 [72] and Chapter 8 [70], Chapter [33].

Functional Requirements

The functional requirement associated with IVR concern maintaining the mechanical strength of the RPV [JAA] during postulated DEC-B conditions through adequate transfer of heat from the corium to containment, ensuring a minimum thickness of RPV [JAA] during DEC-B, thus, maintaining a severe accident safe state.

The CSM [JM01] safety categorised functional requirement applicable to the IVR function is as follows [71]:

- When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall retain corium in the Reactor Vessel Assembly [JAA].

Success Criteria

The IVR subfunction is designed to ensure that the RPV [JAA] remains intact (and containment remains intact through the elimination of ex-vessel phenomena).

Success criteria are presented in Table 15.3-1.

Design Process

The general design process for CSM [JM01] is described in Section 15.5.5.4.2. Parameters informed by analysis include:

- RVCIS flood up flowrate
- Flood up height
- RVCIS initiation timing
- Baffle gap size will be informed by the analysis at DRP3.

The performance of the IVR may also be affected by:

- Coolant chemistry - the impact of coolant chemistry on IVR will be considered in future design phases.
- RPV coatings – the RR SMR has a requirement that the RPV is to be free of any coatings / surface finishes that could have a detrimental effect on CHF.
- Metal content of core/core internals - the RR SMR has a high steel to fuel ratio, this delays core melt and increases the thickness of the core debris light metal layer in the lower head, which influences heat flux through the lower head.
- Oxidation of the RPV – this is not expected to be an issue.

15.5.5.5.3 Severe Accident Depressurisation (SAD) Function

Design information presented for the SAD function is based on DRP1.

Introduction

During a postulated core melt accident (DEC-B) the SAD function can be used to depressurises the RCS [JE] to prevent HPME, DCH, ex-vessel steam explosion and MCCI, which could challenge containment integrity. Depressurisation is also beneficial for interrupting the natural circulation of hot gases in the RCS [JE], which could lead to creep rupture of the RCS [JE] and the SG tubes.

The SAD function has two means to depressurise the vessel via the:

- Manual Depressurisation using the reactor coolant pressure relief system High Temperature Overpressure Protection (HTOP) valves [JEG].
- Manual depressurisation using ADS valves [JNF].

More information on the design of the severe accident depressurisation SSCs, including categorisation and classification, C&I, electrical supplies and operator actions, can be found in Chapter 6 and [57], Chapter 7 [72], Chapter 8 [71] and Chapter [33].

Functional Requirements

The CSM [JM01] safety categorised functional requirement applicable to the SAD concerns the depressurisation of the RCS during postulated DEC-B conditions to prevent the occurrence of HPME and DCH, this is [67]:

- When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce the Reactor Plant [J] pressure.

Success Criteria

The SAD function is used to ensure that the RCS [JE] remains intact.

Success criteria are presented in Table 15.3-1.

Design Process

The general design process for CSM [JM01] is described in Section 15.5.5.4.2. Parameters informed by analysis include:

- HTOP discharge pipework flow capacity
- Low Pressure Emergency Blow Down (EBD) discharge pipework flow capacity
- SAD initiation timing.

Further work is required to substantiate SAD design, sizing and flow capacities by DRP3.

15.5.5.5.4 Hydrogen Reduction System

Design information presented for the HRS is based on DRP1.

Introduction

During postulated DEC-B hydrogen will be generated and released to the containment, hydrogen can be produced from several sources including fuel clad oxidation, steel oxidation, radiolysis, and coolant degassing. Combustion of hydrogen in containment during faults could challenge the integrity of the Containment System [JMA] by the generation of high temperatures and pressures. The HRS [JMT] is sized to remove hydrogen produced from 100 % active clad oxidation. The PARS are fully passive units utilising autocatalytic reactions and as such do not require power.

The Hydrogen Management function relies on the following key SSCs and design features:

- Containment layout – the provision of a sufficient free air volume and an open layout minimising corridors and enclosed space.
- HRS [JMT] – to reduce the mass of hydrogen within the Containment System [JMA].

The lower flammability limit of Hydrogen in containment (in dry air) is 4 %. The maximum concentration to prevent global detonation is 10 % in dry air or 13 % in steam.

More information on the HRS [JMT], including categorisation and classification, C&I, electrical supplies and operator actions can be found in Chapter 6 and [72], Chapter 7 [72], Chapter 8 [71] and Chapter [33].

Functional Requirements

The CSM [JM01] safety categorised functional requirement applicable to the HRS concern the management of hydrogen during postulated DEC-B conditions to protect the integrity of containment, this is [73]:

When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce hydrogen concentrations inside Containment System [JMA].

Success Criteria

The SSCs associated with the HRS are designed to maintain hydrogen concentrations in containment within design conditions during a postulated DEC-B to ensure that the containment remains intact.

Success criteria are presented in Table 15.3-1.

Design Process

The general design process for CSM [JM01] is described in Section 15.5.5.4.2. Parameters informed by analysis include:

- Containment free air volume
- Total Passive Autocatalytic Recombiner (PAR) removal rate
- The mass of hydrogen from fuel clad oxidation
- Position of PARs will be informed by the analysis at DRP2

Future localised analysis will inform the PARs positioning and containment layout design to minimise the risk presented by of localised combustion.

15.5.5.6 DEC-B deterministic analysis

This section presents the results of the DEC-B deterministic analysis performed at RD6 (the inputs to the SAA do not directly align to DRP1, the severe accident SSCs within the model are derived from SDDs produced as part of the RD6 baseline) to demonstrate that in DEC-B the RR SMR can be brought into a controlled state (a severe accident safe state) and the containment function can be maintained to ensure that risks are ALARP. This provides the evidence to substantiate claims made in the safety case, presented in Section 15.11, including:

- The IVR (In Vessel Retention) function will retain core melt in the event of DEC-B.
- The SAD function will avoid a HPME and DCH in the event of a severe accident.

- The HRS will reduce the hydrogen risks associated with in-vessel phenomena to a safe level that will not challenge the integrity of containment in the event of DEC-B.

- The Containment Heat Removal subfunction will provide sufficient cooling/pressure reduction of the containment atmosphere in the event of DEC-B.

The code used to model DEC-B scenarios is the Modular Accident Analysis Program (MAAP), Version 5.06. MAAP is an industry standard SAA specific code with extensive benchmarking and validation underpinning its functions. The code is capable of simulating the reactor and containment response for LWR designs by modelling a wide range of severe accident phenomena, capturing the interactions between the large number of phenomena in a simplified manner. Validation of MAAP is discussed in [74].

RR SMR uses a best estimate approach for modelling severe accidents to ensure predictions are as close as possible to the real-world behaviour, typically supported by sensitivity studies demonstrating an absence of cliff edge effects with variation of the key input parameters.

At RD6 SAA is performed using V1.0.3 of the RR SMR plant parameter file, this version represents the plant's indicative response for a limited range of scenarios. Design assumptions are made within the V1.0.3 parameter file given limitations in the availability of system information. To encompass these uncertainties, some model areas include conservative assumptions until refinements can be made. The level of detail within the model is sufficient to support the analysis approach at RD6 for at power operating states, whilst the plant's remaining operating states (including shutdown states) are to be included in future iterations of the model. In future parameter file iterations development priority will be given to parameters expected to have the most significant effect on the predicted severe accident behaviour, as informed by the ongoing development of the PIRT, Test and Assessment Matrix (TAM) & sensitivity studies. The detail given for these assumptions and the rationale behind them is provided in [75].

The severe accident method follows the VVUQ strategy outlined in [74]. The validation process consists of two key steps: production of a PIRT and TAM. A PIRT highlights the physical phenomena and processes which need to be simulated by the method and ranks them according to their impact on the analysis. A TAM encompasses the assessment of the method adequacy, validation, and uncertainties to demonstrate that for each of the phenomena identified in the PIRT the method is capable of replicating the phenomena at the required level of fidelity and accuracy and the method is sufficiently validated for the phenomena against experimental data which covers the range of application defined in the method requirements. Uncertainties associated with the analysis results produced by the method are required to be understood and quantified to the extent required by the method requirements and analysis methodology. The PIRT [76] and TAM [77] have been produced at RD6, consistent with the MAAP plant parameter file V1.0.2.

Assumptions made at RD6 are discussed in more detail within [78] and summarised below;

- Containment nodalisation – the containment atmosphere is modelled as a large open volume, this limits the potential for the modelling of local temperature effects as well as local hydrogen concentrations. It should be noted that although localised hydrogen conditions are uncertain the global conditions are representative of the open containment design.

- Containment cavity compartment - the RPV [JAA] CHF and therefore the margin between heat flux and CHF are expected to be conservative within the RD6 analysis due to the exclusion of the insulation cooling channel.

- Heat Sinks - the absence of any internal lumped or distributed heat sinks within the model represents an area of conservatism for the prediction of containment pressures and temperatures. Primary circuit heat sinks and externally facing heat sinks are included within the model. The current representation of heat sinks within the model is conservative for peak pressure predictions due to RCS steam release. The heat sinks in containment also provide surfaces for the deposition of fission products released into the containment atmosphere. The limited maturity in the representation of these in MAAP therefore means that fission product movement within containment is not currently considered representative.

While V1.0.3 of the model is a good representation for the analysis at RD6, the model cannot analyse the following:

- Fission product distribution and movement within the containment
- Fission product release to the environment
- Containment failure and containment leakage
- Faults during shutdown or refuelling states
- CCSF
- Emergency Boration System
- ECC [JN01] Recirculation
- PDHR [JN02])
- CSCS
- Secondary Circuit (including steam lines, feed pumps and condenser).

It should be noted that the design of severe accident SSCs described within Section 15.5.5.5 is at DRP1. While severe accident SSCs are captured within the current version of the model at RD6, this is because the analysis lags the design. Severe accident SSC at RD6 is defined within [57]. The main differences in the representation of SSC design in the analysis at RD6 and the design as described above at DRP1 are as follows:

- At RD6 the SAD route is not yet decided, therefore, SAD is modelled in proxy as a delayed 30-minute operator initiation of the ADS, with a flowrate exceeding that expected of future revisions of the SAD function.
- At RD6 the CCSF is not included in the baseline design. At DRP1 CCSF is included as part of the containment heat removal function. Analysis using the RD6 model was used to inform the inclusion at DRP1.
- At RD6 the PCC Heat Exchanger (HX) within the MAAP model are isolated from the LUHS tanks, cooling is established on initiation of the ECC. At DRP1 the PCC HX are not isolated and therefore PCC occurs without delay.
- A reduction in RVCIS [JNM] initial flood-up lines from four at RD6 to two at DRP1, maintaining 1oo2 redundancy. Isolation of recirculation lines and a change in the total

volume of the cavity were also incorporated into the design at DRP1. The net effect is that RD6 base case analysis predicts earlier and faster filling of the cavity than the DRP1 intention. Sensitivity studies carried out at RD6 bound these design changes.

- The hydrogen removal rate of the PARs has been reduced. A sensitivity analysis has been performed at RD6 at the hydrogen removal rate selected at DRP1.

The performance of severe accident SSCs at RD6 has been analysed using three reasonably bounding base cases, with associated sensitivity studies. Performance is assessed with respect to acceptance criteria as described within Table 15.3-1.

The rationale behind the selection of the reasonably bounding severe accident sequences for assessment of the performance of each CSM [JM01] sub function (severe accident mitigative measure) is presented in Table 15.5-3.

Uncertainty analysis and equipment qualification of SSC within CSM [JMO1] will be considered using DRP2.

Table 15.5-3: Accident sequence selection to confirm mitigative measure design provides successful avoidance/mitigation of severe accident phenomena at RD6.

Severe accident phenomena	**Severe accident sequence**	**Severe accident sequence description**	**Rationale**
Containment Heat Removal	LBLOCA with failure of all duty heat removal systems	A double ended guillotine failure of the RCS cold leg.	Provides the greatest demand on short term containment loading (and therefore the heat removal system) during a rapid release of RCS inventory into the containment.
IVR	LBLOCA with failure of all duty heat removal systems	A double ended guillotine failure of the RCS cold leg.	The greatest demand will be placed upon IVR during accident sequences involving rapid core melt progression, this accident sequence results in the highest HF across the lower head.
SAD	SBO	Loss of all AC electrical systems, resulting in the loss of the main coolant pumps and heat removal systems.	This results in a high RCS pressure, selected to demonstrate the expected timing of operation of the SAD function, and impact on sequence progression.
HRS	Slow Depressurisation	A breach within the RCS [JE] with a breach size of 25 mm occurring in the cold leg	The slow depressurisation scenario represents a bounding case for high hydrogen production caused by an extended

Severe accident phenomena	Severe accident sequence	Severe accident sequence description	Rationale
		pipework near the RPV nozzle.	period of cladding coolant interaction.

15.5.5.6.1 Assessment of Containment Heat Removal/Depressurisation of Containment

The effectiveness of the removal of heat and pressure from within containment has been assessed at RD6 to ensure that acceptance conditions are met. This covers the following steps:

- Reasonably bounding accident sequence selection.
- Thermal hydraulic analysis of containment heat removal using MAAP for bounding accident sequences, including sensitivity studies.
- Evaluation of results and comparison with acceptance criteria.
- Analysis of uncertainties (to be considered using DRP2).

Severe accident scenario selection:

Reasonably bounding case at RD6 include:

- LBLOCA with failure of all duty heat removal systems base case.

A description of the initiating event is provided in Table 15.5-3.

During accident conditions, it is generally expected that the greatest demand on short term containment loading (and therefore the heat removal system) is during a rapid release of RCS inventory into the containment. This will occur during a LBLOCA with failure of all duty heat removal systems.

Code Selection

At RD6, MAAP 5.06 is used to determine peak pressure loadings within containment.

Event Description for LBLOCA with failure of all duty heat removal systems at RD6

The sequence progression for a bounding LBLOCA with failure of all duty heat removal systems case:

- Plant operating state (POS) - Mode 1 or 2 (full power).
- LBLOCA - A double ended guillotine failure of the cold leg.
- The RCS [JE] depressurises rapidly into the containment atmosphere. Reactor trip is assumed to be successful.
- The coolant pumps are shut down due to high vibration caused by the loss of coolant.
- CDHR [JN03] and PDHR [JN02] are assumed to fail.

- The RCS [JE] temperature increases, the Core Exit Temperature (CET) increases to 650 °C.
- SAMGs entered, expected DEC-B accident progression, assumed status of SSCs:
- Hydrogen generation begins within the RPV [JAA], hydrogen is released through the RCS break.
- ECC phase 1 [JN01]; ADS [JNF] successful. One accumulator (out of three) is assumed successful when the RPV [JAA] pressure falls below the set point.
- ECC [JN01] phases 2 and 3 do not operate.
- A single train of the PCC/LUHS [JNK] (1oo3) functions upon the initiation of the ECC [JN01] signal. Containment heat removal successful[4].
- RVCIS [JNM] successful, assuming a 30-minute operator delay.
- PARs units remove hydrogen from the containment atmosphere 300 seconds after the containment hydrogen concentration reaches 2 %.
- The core melts and subsequently relocates into the lower head, the RPV lower head is cooled by nucleate boiling of the water in the RPV cavity [UJA].

Acceptance criteria for containment cooling

The acceptance criteria are presented in Table 15.3-1.

Evaluation of results and comparison with acceptance criteria

LBLOCA with failure of all duty heat removal systems base case utilising PCC/LUHS [JNK]

Following the LBLOCA the RPV inventory is quickly discharged into containment through the break. At RD6 PCC begins functioning on initiation of the ECC. The containment pressure rises sharply to ~0.4 MPa(a) and then increases again to ~0.45 MPa(a) once the additional coolant from the accumulator injection has boiled off. Following this the containment pressure increases steadily up to a peak of ~0.5 MPa(a), before decreasing to ~0.43 MPa(a) over the remainder of the 100-hour scenario.

The results of the analysis show that for the bounding base case scenario PCC is effective in controlling containment pressures for the duration of the severe accident scenario. Moreover, the containment pressure was maintained well below the acceptance criteria value of 0.7 MPa(a).

LBLOCA with failure of all duty heat removal systems base case utilising the CCSF.

The CCSF is incorporated into the design at RD7/DRP1 as an alternative active means of depressurising the containment on failure of the PCC/LUHS [JNK], and therefore is not included within SAA performed at RD6. However, additional modelling is performed using the RD6 MAAP model to demonstrate performance of the CCSF.

[4] At RD6 PCC is initiated at the same time as ECC. DRP1 the PCCS utilises a fully wetted system which passively operates immediately, and the CCS is included in the design as an alternative means of containment heat removal.

It is shown that the CCS function is effective in cooling the sump water and limiting the long-term containment pressure rise. However, due to limited heat transfer between the containment atmosphere and sump water pool, a rise in containment pressure is still observed. Nonetheless, peak pressure just exceeds 0.6 MPa(a) after 100 hours, and containment integrity is not expected to be challenged in this period. Spray operation proved effective in quickly reducing containment pressure.

Analysis

The results of the MAAP analysis evaluating the effectiveness of PCC at RD6 for DEC-B can be found in [18].

The results of the MAAP analysis evaluating the effectiveness of CCS at DRP1 (using the RD6 MAAP model) for DEC-B can be found in [79].

Conclusion

The results demonstrate that adequate depressurisation of containment is provided in the event of postulated DEC-B through the operation of PCC/LUHS [JNK] (analysis carried out at RD6) and CCS (analysis caried out using the RD6 MAAP model to inform the design at DRP1 by incorporating an estimate of CCSF operation). Temperature is not currently judged to be a suitable output of this iteration of MAAP analysis and therefore will be included in analysis performed using DRP2.

15.5.5.6.2 Assessment of In Vessel Retention (IVR)

Assessment of the IVR subfunction of the CSM [JM01] is to determine the effectiveness of maintaining RPV [JAA] integrity during postulated DEC-B conditions.

The assessment of the IVR for RR SMR includes:

- Reasonably bounding accident sequence selection.
- Thermal hydraulic analysis within the MAAP model to determine the effectiveness of heat removal from the corium to the containment for bounding accident sequences[5].
- Mechanical stress analysis to establish if the RPV [JAA] has sufficient mechanical strength to maintain RPV [JAA] integrity during DEC-B, this will be presented in Version 3 of the E3S case.
- Evaluation of results and comparison with acceptance criteria.
- Analysis of uncertainties (to be considered using DRP2).

Severe accident scenario selection:

The IVR system is designed to provide cooling to the molten corium through the RPV [JAA] wall, thus ensuring its integrity.

Reasonably bounding case at RD6:

[5] Justification of the CHF claimed within analysis will be presented within a detailed report concerning the evaluation of test data and correlations within literature.

- LBLOCA with failure of all duty heat removal systems base case.

A description of the initiating event is provided in Table 15.5-3.

The greatest demand is placed upon IVR during accident sequences involving rapid core melt progression, this accident sequence results in the highest HF across the lower head. Therefore, at RD6 the LBLOCA with failure of all duty heat removal systems base case is selected as the limiting severe accident scenario for assessing the performance of the IVR.

Code Selection

MAAP analysis is used to determine heat removal (and margin to CHF) from the molten corium to the water within the flooded reactor cavity at angles around the lower head, given reactor cavity water and RPV wall temperatures. MAAP is also used to model ablation of the RPV wall by the molten corium.

An initial structural assessment will be undertaken and reported to support Version 3 of the E3S case using outputs from the MAAP assessment undertaken at RD6.

Event Description

The event description for LBLOCA with failure of all duty heat removal systems is described in Section 15.5.5.6.

Acceptance criteria for IVR

The acceptance criteria are presented in Table 15.3-1.

Evaluation of results and comparison with acceptance criteria

Analysis is performed to calculate the HF of the lower head at a range of angles, this is compared with the CHF (defined as the point at which boiling ceases to be an effective means of transferring heat from a solid surface to water).

It is expected that the reactor cavity is flooded up prior to the relocation of molten corium to the lower head within DEC-B. The results of the SAA at RD6[6] confirm that the reactor cavity is flooded prior to the relocation of molten corium for a LBLOCA with failure of all duty heat removal systems taking into account a 30-minute delay in initiation of the RVCIS [JNM] due to operator action.

The results show that at the most onerous angle for the relative margin between HF and CHF, which aligns with the location of the light metal layer of the molten corium, the analysis shows a significant margin between HF and CHF for the duration of the modelled sequence, lower head temperatures are shown to be controlled long term, slowly decreasing with the decreasing decay heat and containment pressure conditions. These results show that IVR is predicted to be successful for the limiting base case scenario, and as such the acceptance criteria for IVR are met.

Sensitivity studies show that the initiation of IVR can be delayed, however, the RPV Cavity [UJA] must be filled prior to bulk core relocation for IVR to be successful. In the highly unlikely scenario that

---

[6] RVCIS initial flood-up lines have been reduced from four at RD6 to two at DRP1, whilst maintaining 1oo2 redundancy. At DRP1 RVCIS is designed to meet RD6 core relocation times.

no accumulators are available, providing that the IVR is initiated prior to core relocation, IVR is predicted to be successful.

Analysis

The results of the MAAP analysis evaluating the effectiveness of IVR in a severe accident can be found in [18].

Conclusion

The results demonstrate that sufficient cooling of the molten corium within the RPV [JAA] is provided through the operation of IVR during DEC-B. At RD6 all relevant acceptance criteria are met, mechanical stress analysis will be carried out using DRP2.

15.5.5.6.3 Assessment of Severe Accident Depressurisation (SAD)

Assessment of the SAD subfunction of the CSM [JM01] is to determine the effectiveness of depressurisation of the RPV [JAA] during postulated DEC-B, whereby failure of the ECC [JN01] ADS has occurred.

The assessment of the SAD subfunction for RR SMR includes:

- Reasonably bounding accident sequence selection
- Analysis using the MAAP model to determine the effectiveness of RPV depressurisation.
- Evaluation of results and comparison with acceptance criteria.
- Analysis of uncertainties (to be considered using DRP2).

Severe accident scenario selection:

The SAD sub-function is designed to depressurise the RCS [JE], thus ensuring its integrity, preventing high pressure ex-vessel phenomena (HPME and DCH) from occurring.

Reasonably bounding case at RD6:

- SBO base case.

A severe accident sequence which results in a high primary pressure is selected to verify the discharge capability of the SAD function. At RD6 a SBO was determined to be the limiting scenario for assessing the performance of the SAD function.

Code Selection

MAAP 5.06 analysis is used to model severe accident phenomena including pressure conditions within the RCS [JE] and depressurisation rates.

SBO Event Description at RD6

- POS – Mode 1 or 2 (full power).
- A SBO occurs (LOOP, plus loss of all AC power supplies). A loss of power leads to successful reactor trip, but duty heat removal systems fail. Main coolant pumps trip and run down.
- CDHR [JN03] and PDHR [JN02] both fail and the RCS [JE] temperature and pressure increase.
- Hydrogen generation begins within the RPV [JAA].
- RCS [JE] pressure reaches 16 MPa(a) and the ECC [JN01] ADS is initiated, but it fails and RPV [JAA] pressure & temperature continue to increase.
- One train (out of three) of PCC/LUHS [JNK], operates upon the initiation of the ECC signal[7]. Containment heat removal successful.
- RPV [JAA] pressure is maintained between ~16 MPa(a) and ~18 MPa(a) using the SRVs.
- The RPV [JAA] temperature increases, the CET increases to 650 °C.
- SAMGs entered, expected DEC-B accident progression, assumed status of SSCs:
- After a 30-minute delay the operator initiates the SAD system & RVCIS [JNM] to depressurise the vessel and provide water to flood up the reactor cavity to cool the RPV [JAA] lower head and molten corium inside. Valves are on the non-interruptible power supply which are battery backed for 72 hours, and therefore operate in SBO conditions.
- PARs units remove hydrogen from the containment atmosphere 300 seconds after the containment hydrogen concentration reaches 2 %.
- The core melts and subsequently relocates into the lower head, the RPV lower head is cooled by nucleate boiling of the water in the RPV cavity [UJA].

[7] At RD6 PCC is initiated at the same time as ECC. DRP1 the PCCS utilises a fully wetted system which operates immediately, and the CCS is included in the design as an alternative means of containment heat removal.

Acceptance Criteria for SAD Function

The acceptance criteria are presented in Table 15.3-1.

Evaluation of results and comparison with acceptance criteria

Given design maturity at RD6; a decision on the design of the SAD function had not yet been made, therefore the SAD function was not explicitly modelled within RR SMR plant parameter file, the SAD was modelled in proxy instead.

The SBO base case is used in the assessment of SAD function to verify the discharge capability. The performance of the SAD subfunction is assessed through initiation of the ECC [JN01] ADS when a high CET is reached, plus a 30-minute operator delay. It is acknowledged that there will be differences in the flow rates and discharge characteristics between the ECC [JN01] ADS [JNF] route and the SAD HTOP [JEG] route, however, the analysis still provides a good approximation for delayed depressurisation during high pressure faults. Further analysis will be performed using DRP2.

The results show that the expected 30-minute delay in operator initiation of the SAD function does not significantly increase the risk of vessel failure, depressurisation of the RCS occurs significantly before the time when MAAP predicts induced RCS failure in the sensitivity case where SAD is further inhibited.

Analysis

The results of the MAAP analysis evaluating the effectiveness of SAD for DEC-B can be found in [18].

Conclusion

The analysis shows that the SAD function avoids HPME and DCH in the event of DEC-B. If depressurisation occurs within a specified period of time, then induced RCS pipework failure is likely to be avoided, and subsequent mitigative actions such as IVR are likely to be successful. Further work is required to assess the SAD blowdown characteristics.

15.5.5.6.4 Assessment of the Hydrogen Reduction System

The assessment of the hydrogen management system for RR SMR during DEC-B is to determine the effectiveness of the removal of hydrogen from containment to ensure that acceptance conditions are met, this covers the following steps:

- Reasonably bounding accident sequence selection.
- MAAP analysis of hydrogen sources, to aid in the positioning of PARs within containment, this will be carried out using DRP2.
- MAAP analysis to determine global hydrogen concentrations and the global risk of fast deflagration and Deflagration Detonation Transient (DDT).
- Localised analysis of hydrogen (model To Be Confirmed (TBC)) to determine local hydrogen concentrations and the risk of slow deflagration, fast deflagration, and DDT, this will be carried out following DRP3.
- Analysis of uncertainties (to be considered using DRP2).

Sensitivity studies will be performed to reduce uncertainties (using DRP2), uncertainties associated with the HRS include:

- The generation and subsequently the release rate of hydrogen into containment, as this is dependent on fuel coolant interactions and cladding coolant interactions as discussed within Section 15.5.5.3.6. PARs recombination rates are based on 100 % clad oxidation.

- The recombination rate of hydrogen using PARs. This uncertainty is associated with potential deposition or chemical reaction on the PARs surface which inhibits their performance.

Severe accident scenario selection:

The HRS is designed to remove hydrogen from containment.

Reasonably bounding case at RD6:

- Slow depressurisation base case.

The primary hydrogen production mechanism during DEC-B is the interaction between cladding and coolant. When selecting scenarios for MAAP analysis, scoping analysis identified a break size that maximises the period of cladding/steam interaction. Therefore, the chosen break size does not represent a physical pipe break but does provide a reasonably bounding scenario for hydrogen production. The slow depressurisation is therefore selected as the limiting scenario for assessing the performance of the hydrogen management system.

Code Selection

At RD6, MAAP 5.06 is used to determine average global concentrations of hydrogen and assess global flammability, and potential loading on containment.

In addition to global hydrogen analysis using MAAP, detailed localised analysis of hydrogen mixing, and potential for flame acceleration within containment, will be carried out using DRP2. The model that will be used for this analysis is TBC.

Event description for Slow depressurisation case at RD6:

- POS – Mode 1 or 2 (full power).

- A 25 mm LOCA[8] occurs in the cold leg pipework, resulting in coolant loss from the RCS.

- The RCS [JE] depressurises slowly. Reactor trip is assumed to be successful.

- Duty make-up systems do not function, CDHR [JN03]/PDHR [JN02] fail to operate.

- The RCS [JE] temperature increases, the CET increases to 650 °C.

[8] Note that this break size is not based on a real pipe dimension but is selected to generate maximum hydrogen.

- Hydrogen generation begins within the RPV [JAA], hydrogen is released through the RCS break where it is immediately ignited in the containment atmosphere.
- ECC phase 1 [JN01]; ADS [JNF] is successful in depressurising the RCS. One accumulator (out of three) is assumed successful, when the RPV [JAA] pressure falls below the set point. One train (out of three) of PCC/LUHS [JNK], within the analysis scenario, operates upon the initiation of the ECC signal. Containment heat removal successful[9].
- ECC phase 2 and 3 [JN01] do not operate.
- SAMGs entered, expected DEC-B accident progression, assumed status of SSCs:
- RVCIS [JNM] successful, assuming a 30-minute operator delay.
- PARs units retain functionality; however, they do not remove hydrogen due to the prior forced combustion of hydrogen as it is released from the RPV [JAA].
- The core melts and subsequently relocates into the lower head, the RPV lower head is cooled by nucleate boiling of the water in the RPV cavity [UJA].

Acceptance criteria for hydrogen

The acceptance criteria are presented in Table 15.3-1.

Evaluation of results and comparison with acceptance criteria

The analysis results for the limiting base case scenario show that a total of 64 % of the cladding oxidises[10].

Sensitivity case with no PARs operating:

A maximum global hydrogen concentration of 5.2 % is predicted, showing significant margin to the acceptance criteria value.

This peak occurs after the slow depressurisation has already released a significant quantity of the RCS [JE] inventory into the containment and the steam fraction within the containment atmosphere is high (steam has an inerting effect on the flammability of hydrogen).

Opening the ADS [JNF] valve causes an initial rise in hydrogen concentration, and increased release rate of steam from the RCS [JE]. MAAP predicts localised jet combustion of the hydrogen on release. At the time of peak hydrogen concentration, the global steam fraction is 54 %, which then continues to rise and remains above 68 % for the rest of the scenario. The atmosphere is predicted by MAAP to be completely inert above 64 % steam. This means that hydrogen combustion is only possible shortly after the blowdown valve is opened, even when no PARs are functional.

Operation of PARs base case:

[9] At RD6 PCC is initiated at the same time as ECC. At DRP1 the PCCS utilises a fully wetted system which passively operates immediately, and the CCS is included in the design as an alternative means of containment heat removal.
[10] In addition to hydrogen produced from the oxidation of core internals (guide tubes, etc).

The PARs units are assumed to passively begin to warm up once the hydrogen concentration reaches 2 %. There is a 5-minute warm-up period before the PARs begin functioning. Once the PARs units begin functioning the hydrogen concentration within the containment atmosphere begins to drop.

The peak containment hydrogen concentration of 5.2 % and steam concentrations remain the same as the case where no PARs are functional, as this peak occurs shortly after blowdown of the RCS, prior to the removal of hydrogen by PARs. Operation of PARs reduces the hydrogen concentration in containment over time.

The analysis shows that the HRS maintains both peak and long-term global hydrogen concentrations below 4 % (0.04 molar fraction). Analysis demonstrates that acceptance criteria for hydrogen management are met.

Reduced containment steam fraction sensitivity study:

When utilising all three trains of the PCC/LUHS [JNK] with no PARs are available, the average steam fraction only drops to 58 %. The global hydrogen concentration around the time of blowdown is almost identical to the base case and reaches a maximum value of 5.2 %. Over time, the increased number of functional PCC/LUHS [JNK] trains cause a larger reduction in steam fraction and results in an equivalent increase in hydrogen concentration. A peak global hydrogen concentration of 6.2 % occurs at the end of the 100-hour transient during this sensitivity but the total quantity of hydrogen released remains unchanged. The results for this sensitivity study show sufficient margin to the acceptance criteria for global hydrogen concentration.

It is noted that at RD6 it is assumed that the Passive Core Cooling System (PCCS)/LUHS [JNK] begins operating at ~1.7 hours, however, at RD7/DRP1 the PCCS/LUHS [JNK] would operate from the start of transient. During this additional period of heat removal, the containment pressure would be reduced and so would the containment steam fraction. This will increase the potential for hydrogen flammability but is not expected to be challenging for containment integrity due to complete global hydrogen combustion (as demonstrated by the complete combustion sensitivity case). Detailed analysis of localised hydrogen conditions will be used to assess the likelihood of local combustion and potential impact on containment integrity.

Analysis

The results of the MAAP analysis evaluating the effectiveness of HRS during DEC-B at RD6 can be found in [72].

Conclusion

The analysis demonstrates that the hydrogen reduction system reduces the hydrogen risks associated with in-vessel phenomena to a safe level that does not challenge the integrity of containment due to global complete combustion. Global risk of fast deflagration and DDT is not explicitly assessed, but avoidance is demonstrated through avoiding conditions necessary for combustion.

The relevant acceptance criteria are met for the limiting base cases and sensitivity studies assessed at RD6. However, more work is required to:

- Encompass a broader range of scenarios where hydrogen is generated.
- Refine global predictions.

- For localised analysis a detailed analysis method will be developed.

15.5.5.7 Generation of Source Term

Source terms will be generated for accident sequences analysed for DEC-B following DRP3 (using DRP1 and DRP2 design information). The pH of water pools in containment, containment steam conditions and the operation of sprays can affect deposition and absorption rates of the iodine and iodic compounds [80]. Further work is underway to determine the chemistry, and subsequently, the pH and is due to provide initial results for DRP2 which will inform the decision on containment pH control.

15.5.5.8 Analysis of radiological consequences of design extension conditions with core melting

The methodology for conducting severe accident off-site consequence assessments is presented in [81]. This method sets out how the off-site consequences calculations, required to support the Level 3 PSA, will be performed.

Assessment of off-site radiological consequences will be presented following DRP3 (using DRP1 and DRP2 design information). This will be used to provide a comparison against the RR SMR project targets.

15.5.5.9 Demonstration of Practical Elimination

The aim of the practical elimination concept is ‘to complement the adequate implementation of DiD by a focused analysis of those conditions having the potential for unacceptable radiological consequences’ [82].

Event sequences or phenomena which may result in a large or early release will be shown to either be:

- Physically impossible in the design due to inherent safety characteristics of the system or facility.

- Extremely unlikely to occur with a high degree of confidence.

When demonstrating that event sequences are extremely unlikely to occur with a high degree of confidence, the following frequency targets apply:

- The total frequency of events leading to a large or early release shall be less than 1E-06 /yr [5].

- An individual phenomenon or event/fault sequence which can result in a large or early release should have a frequency of occurrence of less than 1E-07 /yr [52].

Where individual phenomena or event/fault sequences are identified that challenge practical elimination targets, design enhancements will be evaluated to meet these targets were reasonably practicable. The overall objective is to ensure risks are ALARP.

An overview of the envisaged approach for demonstrating practical elimination of relevant accident sequences is [83]:

- Step 1 – Identification of relevant phenomena or events that could lead to a large or early release.

- Step 2 – Identification and assessment of safety provision including hazard analysis.
    - Safety provision is identified in the Fault Schedule [84].
    - Assessment of the reliability of safety provision to prevent/mitigate large or early release.
    - The formal assessment of large or early release in the PSA (or by a simpler means where phenomena/events are not included within the available PSA).
- Step 3 – Demonstration that sequences assumed to lead to large or early release are either:
    - Physically impossible or
    - can be considered as 'extremely unlikely with a high degree of confidence'.

Severe accident phenomena, where not deemed impossible by design, will be demonstrated to be managed/mitigated through the provision of design features (incorporated in DiD levels 1-4) making large or early release practically eliminated due to being extremely unlikely to occur with a high degree of confidence.

Both probabilistic (based on frequency targets discussed above) and deterministic (based on design provision) arguments will be provided for event sequences/phenomena deemed to be practically eliminated.

The following phenomena are generically postulated as having the potential to result in a large or early release [85]:

- Rupture of a large pressure-retaining component in the RCS
- DCH
- Fast reactivity insertion accidents
- Large steam explosion
- Detonation of combustible gases
- Containment overpressure (primarily due to long term loss of containment heat removal)
- Basemat penetration or containment bypass during MCCI
- Severe accident with containment bypass
- Significant fuel degradation in a storage fuel pool.

These are judged likely to be residual conditions for which a demonstration of practical elimination will need to be made. Noting that as the design of the RR SMR matures, so will the substantiation of the design; such that some of these conditions may be demonstrated as not contributing to large or early release due to low radiological consequences.

This section provides a summary of the practical elimination arguments for the listed phenomena. A more complete discussion of practical elimination will be provided in [83].

15.5.5.9.1 Rupture of Large Component in the RCS

A large loss of reactor coolant when combined with failure of the containment boundary (for example due to a missile from the original failure) could lead to reactor core damage and consequently contribute to a large and/or early release. Such events are beyond the capability of safety systems and safety features. Instead, demonstration of practical elimination is required, with high confidence that the likelihood of occurrence of such an initiating event would be so low that it can be excluded.

Demonstration of practical elimination of a rupture of a large pressure-retaining component in the reactor coolant RCS integrity and defines the extra activities invoked by the VHR/HR classifications in line with the Categorisation and Classification Method [86], based on acceptance criteria defined in the RR SMR E3S design principles [5]. These classifications apply when the consequences of failure are not acceptable and additional assurance against component failure is required; the definitions are summarised in E3S Case Tier Chapter 23: Structural Integrity [87] as:

- VHR: Structural failure could lead to either an off-site release of dose exceeding 100 mSv or no physical barrier intact to confine any substantial relocation of radioactive material. It is not reasonably practicable to provide control of the resulting conditions either within or beyond the design basis. Failure of such components may lead directly to a large release.

- HR: Structural failure could lead to limited relocation of radioactive material, but with off-site dose limited to less than 100 mSv. It is not reasonably practicable to provide control of the resulting conditions within the design basis; however, it is reasonably practicable to provide BDB defence. Failure of such components may lead to the limited release of radioactive material.

The following components have been identified as potentially containing VHR/HR forgings or welds based on preliminary component assessments following C3.2.2-9 [88]:

- RPV body and closure head
- Pressuriser shell
- SG primary head, tubesheet and secondary shell
- RCP casing
- Reactor coolant loop pipework
- Main steam line pipework
- MSIV body.

It should be noted that VHR/HR classifications are not the preferred route for the prevention of rupture of large component in the RCS, other means are first considered (i.e. prevention of hazards) to reduce risks ALARP.

It is expected that the practical elimination targets for rupture of large components in the RCS will be met and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

15.5.5.9.2 Direct Containment Heating

Rapid accident progression may result in increased pressure within the RCS, if the RCS is not depressurised this could lead to RPV failure. Upon failure of the vessel, molten corium would be forcefully ejected throughout containment creating excess pressure and temperature in the containment atmosphere leading to conditions that would be challenging for containment integrity. This may result in a large and early release.

DiD levels 1-3 (consisting of; duty, preventative, and protective safety measures) ensure CoR, decay heat removal and confinement of radioactive materials such that when they function as designed fuel melt is prevented in fault conditions within the RR SMR for a wide range of different initiating events, including hazards; this includes DEC-A[11]. The following safety measures deliver the CoFT safety function at Level 2 and 3 DiD; condenser based decay heat removal, PDHR, ASD, ECC system and CSCS.

For postulated core melt scenarios, design provision will allow for depressurisation of the RCS. On failure of the ADS (as part of ECC) to provide overpressure protection to the RCS, depressurisation of the RPV can be achieved independently through the SAD Function. For high pressure melt conditions to be realised failure of both means of depressurisation must occur.

It is expected, given design provision within the RR SMR to prevent a core melt, and on occurrence of postulated core melt to prevent subsequent conditions associated with high pressure within the RCS, that the practical elimination targets for high pressure core scenarios are met and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

15.5.5.9.3 Fast Reactivity Insertion Accidents

Fast reactivity accidents can be very energetic and have the potential to destroy the fuel, fuel cladding and other barriers.

The RR SMR will operate with a boron free reactor coolant and, during normal operations, does not require addition of boron to achieve shutdown/holddown. Therefore, a reactivity accident as a result of the initiators associated with boron dilution are not possible, i.e. too little boron addition or dilution of boron through system failure. Fast reactivity insertion accidents via boron dilution are therefore eliminated by physical impossibility of the event sequence.

RR SMR safety measures will limit reactivity excursions. Auto scram and the ASF [JD02] are both delivered by protective safety measures (level 3 DiD) which can be used to shutdown the reactor. The ASF provides an independent, diverse, means of shutting down the reactor to auto scram function. It is expected, given design provision within the RR SMR to limit reactivity excursions, that the practical elimination targets will be met and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

During a severe accident the potentially for re-criticality of the fuel is possible for specific core meltdown scenarios for a short period of time, if the reactor vessel is reflooded with un-borated water in a situation when the control rods have relocated downwards but the fuel rods are yet to relocate. Further work is needed to determine the range of scenarios, and the likelihood and potential consequence of these scenarios; however, it is expected that practical elimination targets

[11] The total CDF associated with the RR SMR is predicted to be 7.56E-07 [102].

will be met and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

15.5.5.9.4 Large Steam Explosions

The interaction between molten corium and water, otherwise known as fuel-coolant interaction, causes the rapid boiling of water to produce large amounts of steam. An energetic fuel-coolant interaction (or steam explosion) can generate a pressure wave which contains sufficient energy to move or deform nearby structures this represents a potentially serious challenge to the integrity of the reactor vessel and/or the containment.

International research demonstrates that the likelihood of in-vessel steam explosions challenging the integrity of the RPV [JAA] is unlikely [55] [56].

Ex-vessel steam explosions may occur if molten core debris is ejected into a flooded reactor cavity after the vessel failure.

The RR SMR is designed to prevent a core melt as discussed in Section 15.5.5.9.2, however, when a core melt is unavoidable, ex-vessel steam explosions are prevented by activating the SAD function (if ADS fails) and containing the corium within the RPV using In-Vessel-Retention (IVR) function.

It is expected, given design provision within the RR SMR to prevent a core melt, and on occurrence of postulated core melt to prevent subsequent conditions associated with large steam explosions, that the practical elimination targets for steam explosion scenarios are met and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

15.5.5.9.5 Detonation of Combustible Gases

During severe accidents, hydrogen can be produced from several sources including fuel clad oxidation, steel oxidation, radiolysis, and coolant degassing. Carbon monoxide combustion is addressed as part of MCCI as described in Section 15.5.5.9.7. Production of meaningful quantities of other combustible gases is physically impossible.

Hydrogen combustion is a very energetic phenomenon. A transition from fast deflagration to detonation of hydrogen would cause a significant threat to the containment integrity.

The RR SMR is designed to prevent a core melt as discussed in Section 15.5.5.9.2, however, when a meltdown is unavoidable, the primary means of preventing hydrogen detonation which could challenge containment integrity is the large open free air volume of the Containment System [JMA] and the intentional layout of SSCs to eliminate corridors and enclosed spaces, where practicable. Local accumulation and stratification are minimised by employing an open layout which promotes mixing by natural circulation during faults. In addition, the HRS [JMT] utilises PARs positioned around containment to recombine hydrogen and oxygen to water.

It is expected, given design provision within the RR SMR to prevent a core melt, and on occurrence of postulated core melt to prevent subsequent conditions associated with a DDT, that the practical elimination targets are met, and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

15.5.5.9.6 Containment Overpressure (Primarily Due to Long Term Loss of Containment Heat Removal)

Where heat produced either by core decay, or molten corium during a severe accident, cannot be removed from containment, overpressurisation and subsequent failure of containment might result.

The RR SMR is designed to prevent a core melt as discussed in Section 15.5.5.9.2, however, when a core melt is unavoidable, the PCC/LUHS [JNK] or the active CCS function can also be used to remove heat from containment.

It is expected, given the RR SMR is designed to prevent a core melt, and on occurrence of postulated core melt to prevent subsequent conditions associated loss of long-term containment heat removal, that the practical elimination targets are met, and such sequences are extremely unlikely to occur with a high degree of confidence. The Level 2 PSA will confirm this.

15.5.5.9.7 Molten Corium Concrete Interaction - Basemat Penetration or Containment Bypass

In a severe accident, if DEC-B design provision has failed, molten corium can melt through the reactor vessel. As a result, containment integrity can be breached in a number of ways:

- Insufficient cooling of the molten core.
- Overpressure failure of containment due to the generation large quantities of non-condensable gases through interactions between the core debris and concrete.

The RR SMR is designed to prevent a core melt as discussed in Section 15.5.5.9.2, however, when a meltdown is unavoidable, the IVR sub-function will retain the molten core inside of the reactor vessel by cooling the reactor vessel from the outside The SAD function will prevent HPME which can also result in MCCI. There are no penetrations in the bottom of the RPV, this removes any weak spots for potential melt through of the molten corium.

It is expected, given design provision within the RR SMR to prevent a core melt, and on occurrence of postulated core melt to prevent subsequent conditions associated with molten core concrete interaction, that practical elimination targets are met, and such sequences are extremely unlikely to occur with a high degree of confidence. This will be confirmed by the Level 2 PSA.

15.5.5.9.8 Severe Accident with Containment Bypass

Containment can be bypassed during a severe accident in a number of ways as described in the following paragraphs.

Failure of lines exiting or entering the containment, this includes an interfacing system LOCA and main steam line rupture, can result in containment bypass if the break is located upstream of the isolation valves. Additionally, SGTR leads to containment bypass, especially if the steam-generator relief valves were to stick open. Such failures could initiate a severe accident or can happen coincidently under accident conditions. It is expected that such containment bypass sequences will be extremely unlikely to occur because most containment penetrations are double isolated. This will be confirmed by the Level 2 PSA. Failure of containment isolation coincident with a severe accident can result in containment bypass. Given design provision within the RR SMR to prevent/mitigate core melt and isolate containment (through the containment isolation function), it is expected that such containment bypass sequences will be extremely unlikely to occur with a high degree of confidence, this will be confirmed by the Level 2 PSA.

Open containment during plant shutdown coincident with accident conditions can result in containment bypass. Severe accident sequences during open containment will be practically eliminated; however, future work is required to determine this. It is expected that such containment bypass sequences will be extremely unlikely to occur with a high degree of confidence, this will be confirmed by the Level 2 PSA.

15.5.5.9.9 Significant Fuel Degradation in a Storage Fuel Pool

To prevent the damage of fuel stored within the storage fuel pool it is necessary to cool and maintain the water level, in addition to maintaining sub-critical conditions. Failure of SFP cooling and top up, or a leak from the SFP, may result in fuel damage to the spent fuel (if spent fuel is exposed to air), this can result in a radioactive release.

It is expected that significant fuel degradation will be practically eliminated through design basis safety measures [89], which will ensure that spent fuel stored in a pool will always be covered by an adequate layer of water and that the fuel remains sub-critical; however, future work is required to confirm this. This will be confirmed by the Level 2 PSA.

15.5.6 Analysis of Spent Fuel Pool Faults

At the time of production of this issue of the E3S case, the design of the SFP safety measures is still being developed. Therefore, only limited and preliminary analysis has been carried out and is summarised in the paragraphs below. Version 3 of the E3S case will provide further results of any analysis conducted.

A preliminary set of PIEs has been defined; these include loss or partial loss of the cooling function and loss of pool inventory. For very frequent faults (DBC-2ii) such as LOOP, where the SFP cooling system can continue its cooling function on both trains, the pool temperature remains below 50 °C. For faults where the FPCS can only continue on a single train (DBC-3i and DBC-3ii), the pool temperature remains below 80 °C. These assessments have been carried out conservatively for hot weather conditions, as the ESWS cooling tower cooling depends on the ambient temperature.

For faults that are even less frequent (DBC-4), the pool heats up to boiling point, and water losses due to evaporation are topped up by gravity feed from the LUHS tanks. The steam is vented to atmosphere via a filtration system. Any leaks from the pools are isolated and contained. The assessment demonstrates that even a fuel assembly that is raised on a FHM can continue to be cooled.

15.5.7 Analysis of Fuel Handling Faults

At the time of production of this issue of the E3S case, the design of the fuel handling safety measures is still being developed. Therefore, only limited and preliminary analysis has been carried out and is summarised in the paragraphs below. Version 3 of the E3S case will provide further results of any analysis conducted.

A preliminary set of PIEs has been defined; these include typical crane faults (such as snagged load or double blocking) that could result in dropped load from or collapse of a handling device such as the Main Overhead Crane (MOC) or a FHM. They also include faults that could lead to inadvertent criticality such as core misload and inadvertently withdrawing the control rods while lifting the Integrated Head Package (IHP) or upper internals.

Assessment and optioneering are ongoing to determine an adequate and sufficient set of Safety Measures such as trips on the MOC and FHM that would stop the lift before a dropped load could occur.

15.5.8 Analysis of Radioactive Releases

15.5.8.1 Design Basis

Analysis of radioactive releases and waste system faults is ongoing and will be reported in a future version of this chapter, which is based on DRP3.

15.5.8.2 Accidents

Assessment of off-site radiological consequences will be presented at DRP3.

15.6 Probabilistic Safety Assessment

15.6.1 General Approach

Both DSA and PSA support the development of the design and the safety case of a nuclear facility. DSA does this by demonstrating that a facility can tolerably respond to identified hazards that define the limits of safe operation. PSA is performed to provide a numerical estimate of risk presented by the facility and provides analysis of alternate scenarios not considered by DSA. PSA can additionally be used to provide insights on the sensitivity of overall facility risks to particular SSC reliabilities and scenarios. The conservative analysis produced by DSA combined with the results of PSA are complementary and together are used to prove the compliance of a facility with safety requirements and acceptance criteria.

The technical requirements on the RR SMR PSA, which are derived from many industry documents defining RGP in the PSA Topic, are laid out in the PSA Technical Requirements [34]. Guidelines for the general development of the RR SMR PSA are laid out in PSA Development Strategy [90]. The PSA Development Strategy also clearly defines where PSA development meets the E3S Level 2 subclaims.

The stated aim of the RR SMR PSA is to demonstrate that nuclear safety risks to workers and the public are understood and acceptable and it is used appropriately throughout the plant lifecycle to manage these risks [90]. This will be substantiated by showing that the RR SMR PSA is: suitable and sufficient to support nuclear safety; used appropriately to support nuclear safety and demonstrates that radiological risks are acceptable and reduced to ALARP.

A large programme of work is planned over several future versions of the RR SMR PSA model to expand its scope and meet its stated aim. This will be documented in future iterations of this E3S Case.

15.6.1.1 Maturity status

Due to the evolving nature of the RR SMR design, the inputs to the PSA presented within this issue of the E3S case do not directly align to one DRP. The safety measures and high-level success criteria are derived from the SDDs produced as part of the RD5 baseline [91]. These were based on version 6 of the Fault Schedule [92] and the version of the RR SMR Definition of PIEs document [93] which were produced using inputs from RD5 with consideration of some subsequent modifications. The next integration of PSA reported in the next issue of this chapter will reflect RD7/DRP1 safety measures and high-level success criteria. The RD5 information used was primarily high-level requirements which did not significantly change in RD6.

Component level information has been derived from system Process & Instrumentation Diagrams (P&IDs) produced as part of the RD6 baseline [94]. The electrical supply information has been derived from Single Line Diagrams also produced as part of the RD6 baseline [94]. The C&I initiation parameters are based on the C&I Engineering Schedule [95] which was additionally produced as part of the RD6 baseline [94]. Updates to the PSA in the next year will bring the systems modelling into alignment with DRP2 ahead of the next issue of this chapter.

15.6.1.2 Scope

The current RR SMR PSA has been developed to evaluate risks inherent in the reactor of the RR SMR design for internal events at power with all relevant systems in their normal duty line up prior to the occurrence of a fault. Where at power is defined as operating modes 1 and 2. The PSA includes ICFs, Loss of Electrics (LoE) faults and Loss of Cooling faults. The initiating fault definition and boundary is as defined in the RR SMR PIEs report [93]. This is a Level 1 PSA which covers the accident phase and quantifies the frequency of occurrence of fuel melt. The PSA only considers sources of radiation in the reactor core.

Future versions of the RR SMR PSA will be extended to include:

- Operations with the reactor shutdown (Modes 3 -6b). (2024)
- Sources of radiation other than the reactor core and RCS, such as the fuel route, fuel storage, and SFP. (2025)
- Consideration of internal and external hazards. (2024 onward)
- Level 2 PSA, meaning coverage of the severe accident phase and quantifying the frequency of radiological release. (2024 onward)
- Level 3 PSA, meaning coverage of the radiological dispersal phase and quantifying the frequency of various health outcomes. (2025 onward)
- Periodic update and validation against the latest reference designs. (ongoing).

The impact of all limitations of scope on the RR SMR PSA risk insights are considered in the PSA Assessment of Limitations [96], which is a companion document to the PSA Main Report [97] and provides context to better aid the interpretation of the analysis and results reported in that document.

15.6.1.3 General Methodology

The RR SMR PSA has been developed to be a best-estimate analysis wherever practicable to do so. This approach is consistent with the PSA Technical Requirements [34] as well as with the wider body of RGP and national and international guidance documents available.

The development of the PSA includes the identification of POS, success criteria and initiating faults and their frequencies, the development of accident sequence progression modelling which are presented in Event Trees (ET)s, and safety measure reliability modelling and operator action modelling as presented in the Fault Trees (FT)s identified in the ETs.

Each of these activities is accompanied by a suite of documentation detailing the method, underpinning assumptions, and data used in the production of each of these elements. Finally, results are quantified, analysed, and documented to inform the design and confirm it adheres to acceptance criteria for the safety case. The methodologies developed for the existing scope of the RR SMR PSA model in each of these elements are presented in the following documents:

- PSA Event Sequence Modelling Methodology [98]
    - This was used as the basis of the Event Sequence Modelling Report [99].

- PSA HBSC Modelling Methodology [100]
    - This was used as the basis of the Operator Actions Modelling Report [101]
- PSA SSC Modelling Methodology [102]
    - This was used as the basis of the SSC Modelling Report [103]
- PSA Data Methodology [104]
    - This was used as the basis of the Data Notebook [105]
- PSA Hazard Event Modelling Methodology [106]
    - This methodology has yet to be used as the basis for any modelling.

Numerous technical assumptions have been made during the development of the RR SMR PSA to capture limitations in the modelling, scope, or availability of information on the project. Each assumption is clearly documented within the relevant modelling documents using an approach explained within the appendices of each of the methodology documents listed previously. This approach includes a priority judgement of the influence of the assumption on risk. Wherever possible, assumptions are intended to be best estimate, consistent with the overall PSA intent to be a best-estimate analysis.

The RR SMR PSA has been constructed using the RiskSpectrum® PSA software. RiskSpectrum® is a well-established PSA software used by over 60 % of the world's nuclear power plants building confidence that it is fit-for-purpose for the RR SMR. The software supports the development of a linked and integrated ET and FT risk model.

Identification of Plant Operating States

POS for the PSA are defined by the Operating Modes set out by the project in the Reactor Island Operating Philosophy [107]. Six operational modes are defined, with three modes having subsets.

1. Power Operations
2. Low Power
3. Hot Standby
4. Hot Shutdown:
    a. Steaming
    b. Non-Steaming
5. Cold Shutdown:
    a. Cold Shutdown Pressurised
    b. Cold Shutdown Depressurised
6. Refuelling.

a. Refuelling with reduced water level above fuel

b. Refuelling with water level above nominal.

Power Operations can be considered as Power Loading (i.e., normal Power Operations), and Low Power (i.e., increasing and decreasing between zero power and low power). These are referred to as Mode 1 and Mode 2 respectively. These two modes are distinct from the shutdown modes as the reactor is operating with at least some control rods withdrawn. They are distinct from each other due to a few key factors especially in that during Mode 1 the reactor is critical and operating at 5 % power or above. Mode 2 is utilised both on the route to Mode 3 or Mode 4 for Shutdown and on return to Mode 1 Power Operations. For much of the reactor life, it will be operating in the Power Loading mode (Mode 1).

As described in Subsection 15.6.1.2 above, the current RR SMR PSA model is limited to operation and faults in Modes 1 and 2. Other modes will be covered in future versions of the RR SMR PSA.

Initiating Event Analysis

At this time, an independent review of possible PIEs separate from the analysis completed by the DSA topic has yet to be carried out. This limitation has been captured and discussed in the PSA Assessment of Limitations [96] as PIE01.

The PIEs identified in the DSA PIE report [93] that are relevant for the scope of the RR SMR PSA are grouped into 3 categories. These are:

- ICF
- Loss of Coolant accident (LOC)
- Loss of Electrics (LOE)

In detail, the PIEs considered in the RR SMR PSA are listed below. Note that ICF.3.2.04 representing Excessive Steam Demand due to SGTR was not modelled in this iteration of the model due to a lack of sufficiently detailed input information, and will be addressed in future versions of the RR SMR PSA.

Table 15.6-1: Postulated Initiating Events and associated Operating Modes in the RR SMR PSA

PIE ID	PIE Description	Applicable Operating Modes	PIE frequency (/yr)
ICF.1.1.01	Complete Loss of Pumped Primary Flow	Modes 1 & 2	{REDACTED}
ICF.1.1.02	Partial Loss of Pumped Primary Flow	Modes 1 & 2	{REDACTED}
ICF.1.1.03	RCP Shaft Seizure	Modes 1 & 2	{REDACTED}
ICF.2.1.01	Primary Pressure Decrease due to Pressuriser Heaters Failing Off	Modes 1 & 2	{REDACTED}
ICF.2.1.02	Primary Pressure Decrease due to Spurious Initiation of Pressuriser Spray	Modes 1 & 2	{REDACTED}

PIE ID	PIE Description	Applicable Operating Modes	PIE frequency (/yr)
ICF.2.1.03	Primary Pressure Decrease due to Failure of CVCS	Modes 1 & 2	{REDACTED}
ICF.2.2.01	Primary Pressure Increase due to Pressuriser Heaters Fail On	Modes 1 & 2	{REDACTED}
ICF.2.2.02	Primary Pressure Increase due to Excessive Operation of CVCS Pre-IET	Modes 1 & 2	{REDACTED}
ICF.2.2.03	Primary Pressure Increase due to Failure to Letdown	Modes 1 & 2	{REDACTED}
ICF.2.2.04	Excessive Primary Pressure due to Spurious Initiation of HPIS	Modes 1 & 2	{REDACTED}
ICF.3.1.01	Spurious Scram	Modes 1 & 2	{REDACTED}
ICF.3.1.02	Reactivity Control Imbalance	Modes 1 & 2	{REDACTED}
ICF.3.1.03	Spurious Initiation of ASF	Modes 1 & 2	{REDACTED}
ICF.3.2.01	Excessive Control Rod Bank Withdrawal	Modes 1 & 2	{REDACTED}
ICF.3.2.02	Excessive Steam Demand due to Large Downstream Steam Leak	Modes 1 & 2	{REDACTED}
ICF.3.2.03	Excessive Steam Demand due to Large Upstream Steam Leak	Modes 1 & 2	{REDACTED}
ICF.3.2.05	Temperature Reduction of Feedwater Supply	Modes 1 & 2	{REDACTED}
ICF.4.1.01	Complete Loss of SG Feed	Modes 1 & 2	{REDACTED}
ICF.4.1.02	Partial Loss of Feed	Modes 1 & 2	{REDACTED}
ICF.4.1.03:_#M1	Complete Loss of Secondary Feed due to Loss of Feed Pumps (Mode 1)	Mode 1	{REDACTED}
ICF.4.1.03:_#M2	Complete Loss of Feed due to Loss of Main Feed Pumps (Mode 2)	Mode 2	{REDACTED}
ICF.4.1.04	Unisolable Feedwater Line Break	Modes 1 & 2	{REDACTED}
ICF.4.2.01:_#M1	Excessive Feedwater Supply (Mode 1)	Mode 1	{REDACTED}
ICF.4.2.01:_#M2	Excessive Feedwater Supply (Mode 2)	Mode 2	{REDACTED}
ICF.5.1.01	Complete Loss of Secondary Heatsink due to the Complete Isolation of Steam Route to Condenser	Modes 1 & 2	{REDACTED}
ICF.5.1.02	Partial Loss of Secondary Heatsink due to Partial Isolation of Steam Route to Condenser	Modes 1 & 2	{REDACTED}
ICF.5.1.03:_#M1	Turbine Trip	Mode 1	{REDACTED}

PIE ID	PIE Description	Applicable Operating Modes	PIE frequency (/yr)
ICF.5.1.04	Complete Loss of Secondary Heatsink due to Spurious SG Isolation via Initiation of PDHR	Modes 1 & 2	{REDACTED}
ICF.5.1.05	Complete Loss of Secondary Heatsink due to Loss of Condenser Vacuum	Modes 1 & 2	{REDACTED}
ICF.5.2.01	Excessive Steam Demand due to Small Downstream Steam Leak	Modes 1 & 2	{REDACTED}
ICF.5.2.02	Excessive Steam Demand due to Small Upstream Steam Leak Pre-IE	Modes 1 & 2	{REDACTED}
LOC.1.1.01	Small Unisolable LOCA in RCS or connecting systems	Modes 1 & 2	{REDACTED}
LOC.1.2.01	Small Isolable LOCA in RCS or connecting systems	Modes 1 & 2	{REDACTED}
LOC.2.1.01	Intermediate Unisolable LOCA in RCS or connecting systems	Modes 1 & 2	{REDACTED}
LOC.2.1.02	LOCA due to SGTR	Modes 1 & 2	{REDACTED}
LOC.2.1.03	LOCA due to Spurious RCS Relief Valve Lift	Modes 1 & 2	{REDACTED}
LOC.2.1.04	Intermediate unisolable LOCA due to Spurious Emergency Core Cooling Initiation	Modes 1 & 2	{REDACTED}
LOC.2.1.05	CRDM LOCA	Modes 1 & 2	{REDACTED}
LOC.2.2.01	Intermediate Isolable LOCA in RCS or connecting systems	Modes 1 & 2	{REDACTED}
LOC.3.1.01	IEF for Large Unisolable LOCA	Modes 1 & 2	{REDACTED}
LOC.3.1.02	IEF for Catastrophic failure of RPV	Modes 1 & 2	{REDACTED}
LOE.1.1.01	IEF for LOOP (24 hours)	Modes 1 & 2	{REDACTED}
LOE.1.1.02	IEF for LOOP (168 hours)	Modes 1 & 2	{REDACTED}

Event Sequence Development

Event Sequence Development is the modelling of the response of the plant, including its C&I systems and operators, to a given situation until a defined end state is reached. Event sequences are described by ETs and start with an initiating event node. An ET graphically models the plant response for the mitigation of PIEs through success or failure of events. These nodes can be a status of safety function, the success or failure of a system or an operator action. Typically, a small ET, large FT structure has been adopted within the Event Sequence Modelling, with support systems typically embedded within the respective FTs rather than explicitly modelled in the ETs.

Event sequences have been derived in line with the Fault Schedule [92] to maintain consistency with current understanding of the plant performance and behaviour. In line with the Event Sequence Methodology [98], best-estimate claims which deviate from the Fault Schedule have been made where possible. This means some sequences make claims on safety functions which may not be claimed by the Fault Schedule and/or which are not always considered available by the DSA. For example, those functions whose safety classification is incompatible with the deterministic safety approach. Where definitive information is unavailable, assumptions have been created and documented. At this stage of the project, transient analysis inputs are not readily available to inform the PSA modelling, and as such blanket assumptions have been made with regards to sequences end states.

Detailed documentation of the modelling performed is provided in the Event Sequence Modelling Report [99].

Success Criteria in the RR SMR PSA

For the development of this issue of the RR SMR PSA, it was assumed that, for all fault sequences, success of at least one safety measure for CoR and success of at least one safety measure for CoFT will result in no fuel damage or degradation. Conversely, it was assumed that failure of all safety measures either for CoR or for CoFT will result in the total melt of all fuel assemblies in the reactor.

Detailed documentation of the success criteria applied to each safety measure within each fault scenario is provided in the Event Sequence Modelling Report [99].

Partial core damage and limited fuel damage end states are not included in the PSA model at this time as the transient analyses detail necessary to be able to determine the extent of fuel damage is yet to be developed. This limitation has been captured and discussed in the PSA Assessment of Limitations [96] as ESC01.

Additionally, an UNDEVELOPED consequence has been created and assigned to specific sequences to represent uncertainty in the design for known aspects. Sequences utilising this consequence are Intermediate Isolable LOCA (on failure of leak isolation), SGTR (on failure to isolate the casualty SG) and Spurious Initiation of the HPIS (on failure of manual and automatic Scram). This follows discussion with relevant stakeholder disciplines, particularly the systems design and plant performance areas, where it was identified that the plant response strategy for these faults is still under development.

These undeveloped sequences have been assessed and further discussed within the PSA Assessment of Limitations [96].

Systems Analysis

The RR SMR PSA models SSCs such that the intended operation of the RR SMR is appropriately represented. The modelling is symmetrical where appropriate and practicable, meaning it considers different plant configurations and loss of different redundant components. The PSA model has a small ET, large FT structure meaning that the Function Events (Fes) represent groups of SSCs fulfilling a common safety function where possible. This is rather than having separate FEs for each system required to fulfil that safety function.

FT modelling has been developed for all SSCs that are claimed in the ETs. SSC-related FEs in the ETs should be linked to a Functional Fault Tree (FFT). The FFTs are distinguished from other FTs in the PSA in that they are linked to FEs and usually have no further upward transfers. The FTs model the success criteria for systems and components to meet their safety function and incorporate the representations of individual component failures, CCFs of similar redundant components, and Operator Actions.

In addition to supporting event sequence and consequence analysis via the ETs, the FTs are presented in a format that can be analysed themselves as stand-alone FT models to estimate the reliability (failure probability) of safety-related systems and support systems.

Support systems such as electrical supplies and signals involved in detection of deviated plant parameters and actuation of safety functions are, so far as is practicable, embedded within the respective FTs rather than explicitly modelled in the ETs. Similarly, Operator Actions are, so far as is practicable, embedded within FTs unless a particular failure alters the progression of the fault sequence.

Systems modelled (fully or partially) as part of the current RR SMR PSA are listed in Table 15.6-2. Many of these are only partially modelled (as their other functions are not relevant to the scope of the PSA analysis) and/or may be modelled with only simplified supercomponent modelling where one failure event represents numerous component failure modes (as more refined component reliability information is either unavailable or not relevant to the scope of the PSA analysis). A supercomponent is a single basic event in the model which represents an entire system or subsystem with a notional failure probability assigned, and which can be modelled in greater detail if shown to be risk significant or more information becomes available.

Detailed documentation of the modelling performed is provided in the SSC Modelling Report [103].

Table 15.6-2: Systems modelled within the RR SMR PSA

Level 1 System Group	Level 2 Systems	RDS-PP Level 3 System/Function
B – Electrical Auxiliary Power Supply Systems	BB – Medium Voltage Electrical Main Supply System 1	BBA – High Voltage Main AC Supply System Unit Boards
		BBT – High Voltage Main AC Supply System Unit Transformer
	BC – Medium Voltage Electrical Main Supply System 2	BCT – High Voltage Main AC Standby Transformer
	BD – Medium Voltage Electrical Supply System for Safety Services	BDA – High Voltage Essential AC Standby Supply System Essential Boards
		BDV – High Voltage Essential AC Standby Supply System AC Power Source
	BF – Low Voltage Electrical Main Supply System 1	BFA – Low Voltage Main AC Supply System for Process Equipment Switchboards
		BFT – Low Voltage Main AC Supply System for Process Equipment Transformer
	BK – Low Voltage Electrical Supply System 1 for Safety Services	BKA – Low Voltage Essential AC Standby Supply System Essential Boards
		BKT – Low Voltage Essential AC Standby Supply System Transformer
		BLA – Low Voltage Essential AC Alternate Supply System Essential Boards

Level 1 System Group	Level 2 Systems	RDS-PP Level 3 System/Function
	BL – Low Voltage Electrical Supply System 2 for Safety Services	BLV – Low Voltage Essential AC Alternate Supply System AC Power Sources
	BM – Uninterruptible Power Supply System	BMA – Low Voltage Uninterruptible AC Supply System Switchboard 1
		BMB – Low Voltage Uninterruptible AC Supply System Switchboard 2
		BMU – Low Voltage Uninterruptible AC Supply System Inverter
	BP – Low Voltage DC Electrical Main Supply System	BPA – Low Voltage Uninterruptible DC Supply System Switchboard
		BPU – Low Voltage Uninterruptible DC Supply System Battery Charger/Rectifier
		BPV – Low Voltage Uninterruptible DC Supply System Batteries
	BK – Low Voltage DC Electrical Supply System 1 for Safety Services	BQA – Low Voltage Uninterruptible DC Supply System for Safety Services Switchboard
		BQU – Low Voltage Uninterruptible DC Supply System for Safety Services Battery Charger/Rectifier
		BQV – Low Voltage Uninterruptible DC Supply System for Safety Services Batteries
J – Nuclear Heat Generation	JD – Reactor Control and Shutdown System	JD01 – Scram
		JD02 – Alternative Shutdown Function
		JDK – Emergency Boron Injection System
	JE – Reactor Coolant System	JEA – Steam Generation System
		JEB – Reactor Coolant Pump System
		JEC – Reactor Coolant System
		JEF – Reactor Pressurising System
		JEG – Reactor Pressure Relief System
	JN – Systems for removal of residual heat from reactor core	JN01 – Emergency Core Cooling
		JN02 – Passive Decay Heat Removal
		JN03 – High Temperature Heat Removal System
		JNB – Passive Steam Condensing System
		JND – High Pressure Injection System
		JNF – Automatic Depressurisation System

Level 1 System Group	Level 2 Systems	RDS-PP Level 3 System/Function
		JNG – Low Pressure Injection System
		JNK – Local Ultimate Heat Sink
	JQ – Hard-wired back-up systems	JQA – Diverse Protection System
	JR – Reactor Protection System	JRA – Reactor Protection System
	JS – Reactor Operational, Protective and Status Limitation System	JSA20 – Reactor Limitation and Preventive Protection System
K – Nuclear Auxiliary System	KA – Component Cooling Systems	KAA – Component Cooling System
	KB – Coolant Treatment	KBA – Level and Volume Control System
		KBE – Coolant Purification System
	KN – Liquid Radioactive Waste Processing System	KNF – Processing and Treatment System for Radioactive Liquid Effluent
L – Steam, Water, Condensate Systems	LA – Feedwater System	LAA – Feedwater System Deaerators
		LAB – Feedwater Piping System
		LAC – Feedwater Pumping System
		LAD – High Pressure Feedwater Heating System
	LB – Steam System	LBA – Main Steam System
		LBK10 – Steam Generator Relief System
		LBK50 – Atmospheric Steam Dump
	LC – Condensate System	LCB – Main Condensate Piping System
		LCC – Main Condensate Pumping System
		LCP – Condensate Storage Tank
		LCQ – Steam Generator Blowdown System
	LJ – Feedwater Supply in case of requirement for Nuclear Steam Generator	LJK –Auxiliary Feedwater System

Level 1 System Group	Level 2 Systems	RDS-PP Level 3 System/Function
M – Systems for conversion of energy (without heat generation) and for transmission of electrical energy	MA – Steam Turbine System	MAG – Condenser System
		MAN – Turbine Bypass System
	MK – Generator System	MKA – Generator System
	MS - Transmission	MSA – Generator Supply Route System
		MST – Generator Transformer

Some systems, such as Heating, Ventilation and Air Conditioning (HVAC) [KL] and Chilled Water System [KJ] are not currently modelled due to lack of sufficient design and system requirements. These will be revisited in each update cycle and included as input becomes available. It is expected that many systems will be added to the scope throughout 2024 due to the work to expand the PSA scope as discussed in section 15.6.1.2. For example, HVAC [KL] and Chilled Water System [KJ] should be represented in the next issue of this Chapter.

Due to the developing maturity of the design, several simplifying assumptions have been applied to the SSC modelling within the RR SMR PSA model. This includes the assumption that SSCs will be tested periodically at precise and constant intervals throughout the plant's operation and three assumed mission times. Typically, SSCs claimed are expected to fulfil their function for 72 hours. The ASD is assumed to be required to provide relief for 3 hours in support of PDHR operation. In an extended LOOP fault, SSCs are required to fulfil their function for an additional 96 hours following the original 72-hour mission time.

A comprehensive accounting and justification of all assumptions is included in the associated modelling reports and in the PSA Assessment of Limitations [96].

Human Reliability Analysis

The approach to Human Reliability Analysis at this issue is addressed in Subsection 15.4.3 of this chapter. Additionally, a thorough review of limitations in this topic area are discussed in the PSA Assessment of Limitations [96].

Detailed documentation of the modelling performed is provided in the Operator Actions Modelling Report [101].

Quantification

Appropriate quantification of frequencies of various end states and associated importance metrics is inherent to the expectation that the RR SMR PSA will provide an assessment of various risk metrics to demonstrate that radiological risks are acceptable. Additionally, quantification of risks and risk contributors form the basis for many of the other applications of the PSA in supporting design and operational decisions, to support nuclear safety throughout the plant lifecycle.

Quantification of the internal events Level 1 PSA provides an estimate of CDF for RR SMR design based on the overall calculated CDF and CDF of each accident sequence. All event sequences and intermediate consequences within the PSA model are quantified to achieve this. This is followed by an appropriate verification of the dominant Minimal Cut-sets (MCSs) from the results of the risk metric quantifications to confirm they are genuine and would actually lead to the associated consequence.

An important task during quantification is the evaluation of uncertainties in the analysis results. All parameters for Basic Events (BE)s and alpha factors are assigned a mean value with no error factors. As such, no parametric uncertainly analysis has been performed on the current RR SMR PSA model. Therefore, uncertainty results for the CDF have not been reported. This limitation does not impact the CDF but means it will be reported with uncertainty bounds in a future version of the model. At this stage, it is expected that the epistemic uncertainties in the other inputs to the PSA such as SSC design and operation and event sequence development will be a more significant source of uncertainty than the aleatory uncertainty of the reliability data. Additionally, the PSA Assessment of Limitations [96] was produced to assess limitations in the analysis and review the effects of those limitations on the PSA analysis results.

Sensitivity studies have been performed to assess the impact of various parameters and ensure the risk conclusions of the PSA are robust. At present, sensitivity studies have been conducted to assess the model sensitivity to data inputs for operator actions, C&I platforms, Scram and electrical supply supercomponents. Sensitivity studies will continue to be performed throughout the lifecycle of the PSA in support of design development, and to verify that the data and methods used are robust. The sensitivity studies performed consider the attributes Sensitivity High and Sensitivity Low for certain BEs within the model, with the analysis considering the impact a change that BE would have on total CDF. Sensitivity High represents the total CDF value if the probability of failure of that BE was ten times higher. Sensitivity Low represents the total CDF value if the probability of failure of that BE was ten times lower. These sensitivities allow analysis to see if the RR SMR design is meeting the high confidence reliability targets, and if it is worth putting more effort in to achieve a lower failure probability.

15.6.1.4 Tools and input data

Software

The RR SMR has been constructed using the RiskSpectrum® PSA software (Version 1.5.3) to develop a linked and integrated ET and FT risk model. As RiskSpectrum® PSA is a well-established PSA software used by over 60 % of the World's Nuclear Power Plants the project has confidence that it is fit-for-purpose for the RR SMR design.

Sources of Data

The RR SMR PSA data inputs are based on industry generic data and international operating experience. Limitations in the PSA model arising from data inputs are assessed in the PSA Assessment of Limitations [96]. The primary sources of generic industry data used for the RR SMR PSA are endorsed by United States NRC and provided as updates by the Idaho National Laboratory. They include industry average parameter estimate data (INL/EXT-21-65055) [108] for physical components in the model and common cause failure parameter estimate data (INL/EXT-21-62940) [109] for CCFs in the model. The Initiating Events Frequencies (IEF)s determined by the DSA topic were used in the current model. The PIE report [93] similarly used sources of generic industry data for initiating events (INL/RPT-23-72818) [110]. Parameters such as mission times, HEPs, component unavailability, and test intervals are based on project assumptions or engineering judgement rather than input from specific sources as much of this information is still under development. All data input to the analysis are documented in the PSA Data Notebook [105]. A high-level summary of each parameter type is summarised below.

- Frequency Parameters are assigned to the PIEs in the PSA and have been taken directly from the Rolls-Royce SMR Definition of PIEs and Derivation of IEF [93]. As the RR SMR PSA currently only includes plant operating modes 1 and 2, the Frequency only includes parameters related to PIEs occurring in these modes. These PIEs and their frequencies are provided in subsection 15.6.1.3.

- Failure Rate Parameters are assigned to the majority of BEs representing component failure modes in the PSA in conjunction with either the test interval model or the mission time model to convert the failure rate to a dimensionless failure probability. Failure rate parameters in the RR SMR PSA have been assigned from the latest 2020 update of the NUREG/CR-6928 (INL/EXT-21-65055) [108] to make best use of recent operational experience. This latest 2020 update does not always include average demand frequency data for components. In these cases, values have been taken from the industry average baselines tables.

- Probability Parameters are typically assigned to BEs in the PSA where it is not appropriate or practical to assign a failure rate in conjunction with a mission time or test interval parameter. These are based on engineering judgment to determine the value used in the model. Examples include data assigned to BEs representing:

    - Components involving software or firmware failures.

    - Proportions of the year spent in a particular plant operating mode or configuration.

    - Unavailability of a component due to maintenance or testing.

    - Components failing to operate on demand where it may have been demonstrated that reliability is insensitive to test frequency, or where there is a lack of suitable failure rate data available.

- CCF Parameters are assigned using Alpha factor CCF analysis carried out at the component level. At this time 'pooled' alpha factor parameters have been sourced from the Idaho National Laboratory (INL/EXT-21-62940) [109] for all active redundant component types.

- Test Interval Parameters are assigned in conjunction with a failure rate to BEs representing components failing to operate on demand. The EMIT schedule for the RR SMR is still under development. The rationale behind the test intervals currently assigned to BEs in the RR SMR PSA model are documented in Section 2.9 of the Data Methodology Report [2].

Table 15.6-3:Test Interval Parameters

Parameter ID	Parameter Description	Numerical Value (hours)
TI-1000	Test Interval 1000 hours	1.00E+03
TI-200	Test Interval 200 hours	2.00E+02

Parameter ID	Parameter Description	Numerical Value (hours)
TI-20000	Test Interval 20000 hours	2.00E+04
TI-2500	Test Interval 2500 hours	2.50E+03
TI-400	Test Interval 400 hours	4.00E+02
TI-5000	Test Interval 5000 hours	5.00E+03

- Mission Time parameters are assigned in conjunction with a failure rate to BEs representing components failing to operate over a defined period. The RR SMR project has generally adopted a 72-hour mission time although other mission times are applied to BEs that represent SSCs providing certain functions (e.g. ASD) or following specific faults (e.g. Extended LOOP).

Table 15.6-4: Mission Time Parameters

Parameter ID	Parameter Description	Numerical Value (hours)
3_HOURS	3-hour mission time	3.00E+00
72_HOURS	72-hour mission time	7.20E+01
96_HOURS	96-hour mission time for extended loss of grid (168 hours)	9.60E+01

15.6.2 Results of the Level 1 PSA

This section summarises the results produced within the PSA area. PSA results are presented in the PSA Main Report [97], which is complimented by the PSA Assessment of Limitations [96]. Together they present frequencies for overall fuel melt with contributions by initiating events, key risk sequences, top minimal cutsets, selected sensitivity studies and associated uncertainties.

The overall, or total, CDF from the PSA model is calculated as {REDACTED} per reactor year (pry) of power operation. This is a factor of {REDACTED}x larger than the RR SMR CDF design target (1E-07 pry), see Subsection 15.3.2 above. This result has been derived with significant scope limitations in the PSA, as well as undeveloped sequences and modelling. A further, more detailed comparison of the result against target metrics is made within the PSA Assessment of Limitations [96].

Contribution of Initiating Events to CDF

The contributions of the Initiating Event fault categories to total CDF are shown below:

Table 15.6-5: Initiating Event Fault Categories

Fault Category	Fault Category Description	No. of PIEs	Fractional Contribution (FC)
ICF.1.x.x	Flow-related faults	3	1 %
ICF.2.x.x	Pressure-related faults	7	4 %
ICF.3.x.x	Reactivity-related faults	7	20 %
ICF.4.x.x	Feed-related faults	5	13 %
ICF.5.x.x	Heatsink-related faults	7	6 %
LOC.1.x.x	Small LOCA	2	~0 %
LOC.2.x.x	Intermediate LOCA	6	20 %
LOC.3.x.x	Large LOCA	2	1 %
LOE.1.x.x	Loss of Electrics	2	34 %

The LOE faults (LOE.1.x.x) are the most significant contributors, with a FC of approximately 34 % to the total CDF. Note that there are only two related fault sequences for this category. The most significant contribution comes from the extended loss of grid fault (LOE.1.1.02).

Intermediate LOCAs (LOC.2.x.x) and Reactivity-related faults (ICF.3.x.x) form the next highest risk categories, each with a Fault Contribution (FC) of 20 % to the total CDF. Spurious Scram (ICF.3.1.01) and Spurious ASF (ICF.3.1.03) contain most of the risk associated with the reactivity-related faults. SGTR (LOC.2.1.02), Spurious RCS Relief Valve Lift (LOC.2.1.03) and CRDM LOCA (LOC.2.1.05) present the highest level of risk for the Intermediate LOCAs.

Feed-related faults provided a FC of 13 % to the total CDF. Of the 5 feed-related faults, Partial Loss of SG Feed (ICF.4.1.02) was found to be the highest-risk PIE with Excessive Feedwater Supply (ICF.4.2.01) also identified as a PIE of concern.

Key Risk Sequences

The key risk sequences identified at this stage of the design are provided below, with discussion and suggested improvements to the model or plant design. Each sequence is described based on the claimed Function Events from the PSA Model. A sequence was considered to be Key-Risk if its frequency was equal or higher than 5 % of the RR SMR Design Target. Therefore, all presented Key-Risk Sequences have frequency equal or higher than 5.00E-9 pry.

It should be noted that each of these sequences is individually examined in Section 4 of the PSA Assessment of Limitations [96] to assess how they may have been affected by limitations in the model. Section 4 assesses the top 19 sequences to understand the impact of identified limitations, how modelling may evolve and what the quantitative impact of resolving the limitations might be. Evaluations of these limitations indicate that the frequency results for the two top sequences discussed below are likely to be conservative and that these may be reduced as the limitations are addressed and modelling evolves.

Table 15.6-6: Key Risk Sequences

Sequence No.	Sequence	Sequence Description	Frequency (pry)	FC (%)
1	LOE.1.1.02:_#M1_~2_#02:0010	LOOP 168 hours (following 96 hours)	{REDACTED}	33 %
2	ICF.3.1.03:_#M1_~2_#01:0023	Spurious Initiation of ASF	{REDACTED}	13 %
3	ICF.4.1.02:_#M1_~2_#01:0006	Partial Loss of SG Feed	{REDACTED}	9 %
4	LOC.2.1.03:_#M1_~2_#01:0002	Spurious RCS Relief Valve lift	{REDACTED}	6 %
5	LOC.2.1.02:_#M1_~2_#01:0002	SGTR	{REDACTED}	5 %
6	ICF.3.1.01:_#M1_~2_#01:0021	Spurious Scram	{REDACTED}	4 %
7	LOC.2.1.02:_#M1_~2_#01:0010	SGTR	{REDACTED}	4 %
8	LOC.2.1.05:_#M1_~2_#01:0002	CRDM LOCA	{REDACTED}	3 %
9	ICF.2.2.04:_#M1_~2_#01:0007	Spurious Initiation of HPIS	{REDACTED}	2 %
10	ICF.5.1.03:_#M1_#01:0022	Turbine Trip	{REDACTED}	2 %
11	ICF.2.2.04:_#M1_~2_#01:0011	Spurious Initiation of HPIS	{REDACTED}	2 %
12	LOC.3.1.02:_#M1_~2_#01:0001	RPV Failure	{REDACTED}	1 %
13	LOC.2.1.03:_#M1_~2_#01:0003	Spurious RCS Relief Valve lift	{REDACTED}	1 %
14	ICF.1.1.02:_#M1_~2_#01:0022	Partial Loss of Flow	{REDACTED}	1 %
15	ICF.5.1.05:_#M1_~2_#01:0016	Loss of Condenser Vacuum	{REDACTED}	1 %
16	ICF.4.1.02:_#M1_~2_#01:0015	Partial Loss of SG Feed	{REDACTED}	1 %
17	ICF.3.1.03:_#M1_~2_#01:0003	Spurious Initiation of ASF	{REDACTED}	1 %
18	ICF.4.2.01:_#M1_#01:0022	Excessive Feedwater Supply (Mode 1)	{REDACTED}	1 %
19	ICF.4.1.02:_#M1_~2_#01:0019	Partial Loss of SG Feed	{REDACTED}	1 %
	Other Sequences		{REDACTED}	9 %
	TOTAL		{REDACTED}	**100 %**

Sequence 1, LOE.1.1.02:_#M1_~2_#02:0010, has a frequency of {REDACTED}, which contributes 33 % to the total CDF for all sequences. This sequence represents the case of a LOOP of 168 hours and failure of the House Load Generator wherein the operator fails to maintain Diesel Generator (DG) Fuel Tank levels beyond 72 hours, leading to a failure of standby AC generators to provide power. Under these circumstances, it is assumed that fuel melt will occur due to a failure to provide decay heat removal. The most significant contributor to this sequence is failure of the operator to complete the action of manually maintaining the DG Fuel tank levels beyond 72 hours.

As noted in the Assessment of Limitations [96], limitation SCR05, which refers to assumptions that result in the model not crediting that decay heat is significantly lower beyond 72 hours post trip, means that primary circuit pressures and temperatures could be much lower such that core damage might not occur following failure of some safety functions and that operator action grace periods might be significantly longer. There is also an implicit assumption made in the assignment of the success consequence following the loss of all electrical supplies which is that electrical power is necessary after 72 hours to prevent core damage. In reality, decay heat removal via PDHR or ECC would already have been aligned before the loss of electrical supplies and both of these means of decay heat removal use natural convection rather than pumped coolant flow to core the reactor.

Additionally, limitation HSC07 refers to the assumption that the LUHS tank provides sufficient inventory for 72 hours of cooling for ECC. Once exhausted the model assumes that an active pump is required to replenish this resource. Since this assumption was made, the LUHS design has evolved to provide additional level of inventory.

Disregarding the limitations of the event sequence as discussed above, the current configuration of the sequence is dependent on the failure of an operator action. Note that an assumed conservative approach was used for the modelling of Operator Actions, as sufficient data to derive best-estimate HEPs was not yet available. As such, in line with Assumption PSA-AS-OPA-001 [101], each operator action HEP was assigned a screening value of 1E-02. This is particularly relevant to this operator action due to the long grace period, and as such the operator has a notable amount of time to diagnose the situation and prepare to perform this action. This assumption introduces conservatism into this fault and will be revised as Human Reliability Assessment (HRA) inputs become available to support a best-estimate approach on operator actions.

Sequence 2, ICF.3.1.03:_#M1_~2_#01:0023, has a frequency of {REDACTED}, which contributes 13 % to the total CDF for all sequences. This sequence represents the case of Spurious Initiation of ASF wherein both manual and automatic scram fails. Under these circumstances, it is assumed that fuel melt will occur due to a failure of reactivity control. The most significant contributor to this sequence is failure of the control rods to insert.

As noted in the Assessment of Limitations [96], due to uncertainty about the nature of the spurious actuation, the current modelling takes the bounding case: the spurious actuation of ASF causes a reactivity transient requiring shutdown; however, this ASF actuation does not provide sufficient anti-reactivity to ensure a shutdown and also renders the ASF unavailable in the long term. It is expected that this case is conservative and that the PIE will be better defined and perhaps divided into several PIEs according to the exact effects and variants of the postulated transient allowing a more through and best estimate evaluation of ASF.

Additionally, as the ASF has already malfunctioned, it is treated as unavailable for this fault in line with Assumption PSA-AS-ESD-048 [99]. No credit is given for reactivity decrease due to Spurious Initiation of ASF, as it is expected that, in the bounding case, injection of boron has failed. As such, an N-1 rod requirement has been placed on Scram in line with Assumption PSA-AS-ESD-051 [99]. This is captured in the Assessment of Limitations [96] as limitation SCR04. The HPIS is also assumed to be unavailable, as it must malfunction as part of Spurious Initiation of ASF in line with Assumption PSA-AS-ESD-050. These assumptions introduce conservatism into this fault and may be revised as transient analysis inputs become available to support a best-estimate approach, and as the C&I Engineering and System Design team work on the plant response to this fault.

Key Risk Minimal Cut-sets (MCSs)

The most significant MCSs have been analysed to understand the risk associated the key factors within the design contributing to risk. A MCS was considered to be Key-Risk if it has a fuel melt consequence, and if its frequency is equal or higher than 5 % of the RR SMR Design Target. Therefore, Key-Risk MCSs will have frequency equal to or higher than 5.00E-9 pry.

Table 15.6-7: Key Risk MCSs

MCS No.	Probability (pry)	FC	Sequence Description
1	{REDACTED}	33.10 %	168-hour LOOP followed by: • Failure to stabilise on House Load • Failure to refuel standby AC generators/Failure to top up water sources post 72 hours
2	{REDACTED}	13.20 %	Spurious Initiation of ASF, followed by: • Reactor shutdown scram fails on demand due to mechanical fault (2 or more rods fail to insert)
3	{REDACTED}	3.17 %	Spurious Scram, followed by: • HDPS Platform fails on demand • RPS platform fails on demand
4	{REDACTED}	1.90 %	Spurious RCS Relief Valve lift, followed by: • PCC Heat Exchanger loss of heat transfer CCF
5	{REDACTED}	1.54 %	SGTR occurs in SG2, followed by: • RPS system fails to configure HPIS • Operator fails to configure HPIS
6	{REDACTED}	1.54 %	SGTR occurs in SG3, followed by: • RPS system fails to configure HPIS • Operator fails to configure HPIS
7	{REDACTED}	1.54 %	SGTR occurs in SG1, followed by: • RPS system fails to configure HPIS • Operator fails to configure HPIS
8	{REDACTED}	1.40 %	SGTR occurs in SG3, followed by: • ECC gravity drain refuelling pool strainer plugging CCF
9	{REDACTED}	1.40 %	SGTR occurs in SG1, followed by: • ECC gravity drain refuelling pool strainer plugging CCF
10	{REDACTED}	1.40 %	SGTR occurs in SG2, followed by: • ECC gravity drain refuelling pool strainer plugging CCF
11	{REDACTED}	1.32 %	Catastrophic failure of RPV

MCS No.	Probability (pry)	FC	Sequence Description
12	{REDACTED}	1.18 %	Spurious RCS Relief Valve lift, followed by: • Reactor shutdown scram fails on demand due to mechanical fault (2 or more rods fail to insert)
13	{REDACTED}	1.07 %	Spurious RCS Relief Valve lift, followed by: • ECC containment sump strainer plugging CCF
14	{REDACTED}	1.07 %	Spurious RCS Relief Valve lift, followed by: • ECC gravity drain refuelling pool strainer plugging CCF
15	{REDACTED}	0.88 %	Partial Loss of Feedwater (to SGs 1 and 2), followed by: • HDPS platform fails on demand • RPS platform fails on demand
16	{REDACTED}	0.88 %	Partial Loss of Feedwater (to SGs 2 and 3), followed by: • HDPS platform fails on demand • RPS platform fails on demand
17	{REDACTED}	0.88 %	Partial Loss of Feedwater (to SGs 1 and 3), followed by: • HDPS platform fails on demand • RPS platform fails on demand
18	{REDACTED}	0.77 %	Loss of Condenser Vacuum, followed by: • HDPS platform fails on demand • RPS platform fails on demand

MCS 1 has a frequency of {REDACTED} and contributes 33.1 % to the failure probability of all sequences. This MCS is caused by failure of the operator to maintain DG Fuel Tank levels beyond 72 hours following a failure of the House Load Generator to run following LOOP.

The events included in MCS 1 are:

- LOE.1.1.02:_#M1_~2_#00 – LOOP Pre-IE
- DGFUEL:01#H#4#TOP_UP – Operators fail to maintain DG fuel tank levels beyond 72 hours
- MKA01_HLOAD_FAIL:XXX_XXX – House Load Generator fails to run following LOOP

This MCS is subject to uncertainty as the frequency of occurrence of this PIE is effectively a single expert judgement. In addition to this, all HEPs have been assigned a basic screening value of 1E-02 in line with Assumption PSA-AS-OPA-001 [101]. It is an assumed conservative assumption for an extended loss of grid, as the operator has several days to correctly assess this fault and prepare for any actions. The probability of the House Load Generator failing to run has also been assigned a value based on engineering judgement. Values derived using engineering judgement have been highlighted within the PSA Issues Log [111] as requiring further review with relevant disciplines.

MCS 2 has a frequency of {REDACTED} and contributes 13.2 % to the failure probability of all sequences. This MCS is caused by mechanical failure of Scram following a Spurious Initiation of ASF fault.

The events included in MCS 2 are:

- ICF.3.1.03:_#M1_~2_#01 –Spurious Initiation of ASF
- JD01X_SCRAM_N-1:XXX_XXX – Reactor shutdown scram fails on demand due to mechanical fault (2 or more rods fail to insert)

As the ASF has already malfunctioned, it is treated as unavailable for this fault in line with Assumption PSA-AS-ESD-050 [99]. No credit is given for reactivity decrease due to Spurious Initiation of ASF as it is expected that in the bounding case, injection of boron has failed. As such, an N-1 rod requirement has been placed on Scram in line with Assumption PSA-AS-ESD-051 [99]. This introduces conservatism into this fault as it is expected that Spurious ASF initiation would result in a reactivity decrease.

HRA Sensitivity Study

A sensitivity analysis has been performed for all operator actions. Due to the assumed conservative approach to the HEPs used in the model for each of the operator actions, in line with Assumption PSA-AS-OPA-001 [101].

Table 15.6-8: Operator Actions CDF Values for different Sensitivity Values

Description	Sens. High (pry)	Sens. Low (pry)
Operators maintain DG fuel tank levels beyond 72 hours	{REDACTED}	{REDACTED}
Manual HPIS configuration in case of SGTR	{REDACTED}	{REDACTED}
Manual CVCS Restart	{REDACTED}	{REDACTED}
Manual HPIS stop in case of Spurious HPIS Initiation	{REDACTED}	{REDACTED}
Manual scram on observation of reduction in feedwater flow rate or SG level	{REDACTED}	{REDACTED}
Manual scram on small downstream steam leak	{REDACTED}	{REDACTED}
Reactor power reduced to 70% to allow CDHR to operate indefinitely	{REDACTED}	{REDACTED}
Manual scram on rod out of position alarm	{REDACTED}	{REDACTED}
Manual leak isolation	{REDACTED}	{REDACTED}
PDHR provided for 96 hours with LUHS top-up	{REDACTED}	{REDACTED}
Manual CVCS Stop	{REDACTED}	{REDACTED}
Manual scram on observation of depletion of boron tank.	{REDACTED}	{REDACTED}
Manual Scram/Controlled shutdown on detection of leak	{REDACTED}	{REDACTED}

Description	Sens. High (pry)	Sens. Low (pry)
Manual spray isolation and heaters on with 1oo2 spray lines isolated	{REDACTED}	{REDACTED}
Manual scram on high pressure alert	{REDACTED}	{REDACTED}
Manual heater restart on low pressure alert	{REDACTED}	{REDACTED}
Manual ASF on failure of Scram (Pressure Reduction)	{REDACTED}	{REDACTED}
Manual heater trip on high pressure alert	{REDACTED}	{REDACTED}
Manual scram on low pressure alert	{REDACTED}	{REDACTED}
Manual ASF on failure of Scram (Loss of Feed)	{REDACTED}	{REDACTED}

The top four operator actions show the most significant change in CDF following a change in their respective HEP, as represented by their Sensitivity High and Sensitivity Low values. The remaining operator actions have the Sensitivity High and Sensitivity Low values approximating the current CDF ({REDACTED}pry). This means that the change of HEP in these actions does not significantly impact the CDF.

15.6.3 Results of the Level 2 PSA

As discussed in Subsection 15.6.1.2 above, the Level 2 PSA has yet to be developed for the RR SMR design. Development of this aspect of the PSA will require interactions and cross working with the Severe Accidents topic (see relevant parts of Subsection 15.5). The Level 2 PSA will be developed in the next year following DRP2 and the results will be presented in the next version of the E3S Case.

The previous issue of this E3S Chapter 15 noted that the Level 2 PSA overall Large Release Frequency (LRF) from all reactor plant events was calculated as {REDACTED} of power operation and was based on analysis performed in 2021 [112]. This represented an earlier version of the RR SMR PSA model which was used for preliminary concept design development and optioneering. The relevance of the information used at that time to the present design is limited and any inference from this result should be limited as well.

Without a Level 2 PSA it is not possible to determine the overall LRF for the RR SMR design at this present time. Hence, comparison against the RR SMR numerical target for this frequency of 1E-08 pa is also not possible (Subsection 15.3.2). However, based on the relative similarity of the reactor type and intended operation of the RR SMR to comparable existing units in the nuclear industry, no anticipated unique scenarios are anticipated that would produce values from the Level 2 PSA that would not be comparable to or meet this RR SMR numerical target.

This limitation has been captured and discussed in the PSA Assessment of Limitations [96] as SAC01.

15.6.4 Results of the Level 3 PSA

As discussed in Subsection 15.6.1.2 above, the Level 3 PSA has yet to be developed for the RR SMR design. The Level 3 PSA is expected in a limited form following DRP3 to support a future iteration of E3S Chapter 15. Development of this aspect of the PSA will require interactions and cross working with the Radiological Consequences area. There are clear limitations in relation to site-specific aspects of the Radiological Consequences analysis and therefore the Level 3 PSA to support the Generic E3S case will also be limited.

Without a Level 3 PSA it is not possible to determine the frequency of radiation exposure from accidents to individuals on-site, individuals off-site and the wider population from the RR SMR design at this present time. Hence, any comparison against the RR SMR numerical targets for these frequencies ranging between 1E-03 and 1E-07 pa for various scenarios are also not possible (Subsection 15.3.2). However, based on the relative similarity of the reactor type and intended operation of the RR SMR to comparable existing units in the nuclear industry, no anticipated unique scenarios are anticipated that would produce values from the Level 3 PSA that would not be comparable to or meet these RR SMR numerical targets.

This limitation has been captured and discussed in the PSA Assessment of Limitations [96] as RDC01.

15.6.5 PSA Insights and Applications

Recognising the impact of assumptions necessitated by the level of detail present in the design have on the insights to be gained by the model, the key insights of the PSA include:

- The overall, or total, CDF from the PSA model, which is calculated as {REDACTED} pry of power operation.
- The Initiating Event fault categories contributing to the CDF in the current model in order of significance include:
    - LOE faults (LOE.1.x.x), with a FC of approximately 34 % to the total CDF.
    - Intermediate LOCAs (LOC.2.x.x) and Reactivity-related faults (ICF.3.x.x) form the next highest risk categories, each with a FC of 20 % to the total CDF.
    - The remainder of the ICF fault categories make up the remaining FC of 26 % to the total CDF.
- The identification of key risk contributors inherent in the design, but not attributed to a single sequence or BE. These include CCFs, Operator Actions, and Supercomponents. Identifying the contribution of each of these aspects to the overall risk profile from the PSA model will aid the understanding of where diversity should be improved within the design, in the definition of operator procedures, and in identifying where a high level of confidence may be required in values assigned to supercomponents.
- The critical review of the assumptions used and the current modelling results highlight areas to focus on refinement in future work.

Alongside the full complement of tools used to ensure an RR SMR design with risks that are demonstrably ALARP, the PSA is being applied to ensure that design options being considered:

- Achieve a CDF design target of <1E-07 /yr.
- Demonstrate that the risk in the design and operation of RR SMR units can be considered ALARP.

- Are optimised for reliability – importance analysis is used to inform safety measure design evolution: number, type, capability and degree of redundancy (number of trains) for each safety measure.

- Achieve a balanced and optimised design, so that no particular class of accident or reactor feature makes a disproportionate contribution to the overall risk, and to support risk minimisation of the design.

- Assures any dependence between safety measures, SSCs does not undermine Design Basis Accident risk conclusions.

The considerations listed above are fed back to the design engineers to further improve the design. This is accomplished through informal sessions with specific system designers and formal transmittal of PSA results. Optioneering requests are processed by the PSA engineers to provide risk insights of proposed design options.

Other PSA applications will be realised as the RR SMR design progresses throughout the plant lifecycle, such as the use of PSA to risk inform EMIT activities, OLCs and emergency planning.

15.7 Internal Hazards Analysis

15.7.1 Overview

The underpinning safety aim for the RR SMR is an inherently safe design. Safety will be demonstrated in the design and the design will provide tolerance to hazards (and events), such that if a hazard were to occur, the plant is able to reach a safe and stable state and the risk to nuclear safety is ALARP. Internal hazards expertise is provided as the design develops to inform design decisions which improve the inherent level of safety within the plant. The RR SMR Internal Hazards Strategy outlines this approach [113].

The general approach to addressing internal hazards within the RR SMR is to prevent internal hazards occurring in the first instance by design. Where this is unpracticable, the approach is to segregate redundant trains of safety systems that perform each of the plant safety functions. Where practical, the aim is to provide 'divisional segregation' of safety trains, i.e. splitting areas of the plant into separate divisional areas containing a train of each safety system. Where segregation is not practical, i.e. where there are exceptions to segregation, then SSCs will need to be demonstrated to withstand hazards, or local protection will need to be provided. Further discussion on segregation strategy is provided in the internal hazards strategy [113].

The overall layout of the plant and equipment is being optimised to eliminate or minimise the impact of internal hazards. The direct effects of internal hazards on SSC and any interactions between a failed SSC and other SSC will be minimised. The Architectural and Layout Summary Report [114] demonstrates the consideration of internal hazards into the overall layout. Internal hazard reviews of the layout have been undertaken at an early stage to inform the design, see 15.7.3 (approach). This process is described in the internal hazards strategy [113].

The Internal Hazards Methodology [115] summarises the analysis methods to be used in the assessment of internal hazards for the RR SMR. The internal hazards analysis is performed according to the methodology as far as possible, however, where design maturity is limited, assumptions are made to inform the analysis.

The baseline design for the Internal Hazards analysis for RR SMR E3S Case Version 2 for Reactor Island (within Hazard Shield) is the design prior to DRP1 (RD6) and DRP1 is the baseline design for Outside the Hazard Shield. The Internal Hazards Summary Report - Reactor Island within Hazard Shield [116] is based on RD6 due to length of time it takes to conduct the analysis. For the Internal Hazards Summary Report – Outside Hazard Shield [117] the design maturity is relatively low in comparison to Reactor Island.

For areas inside and outside the hazard shield, the layout has been thoroughly screened for potential internal hazards. Where limitations of layout have been identified, safety measures have been identified to minimise the impact of faults/ internal hazards.

15.7.2 List of Internal Hazards

15.7.2.1 Individual Internal Hazards

As per the Internal Hazards Strategy [113] the individual internal hazards that have been considered in the analysis are displayed in Table 15.7-1 below.

Table 15.7-1: Individual Internal Hazards

Individual Hazard	Definition
Fire	The internal fire hazards considered are: • Building/solid material fire • Oil or other liquid pool fires • Gaseous fires
Explosion	The explosion hazards considered are: • Explosions/blast following internal arcing faults. • Hydrogen Explosions. • Flammable Explosions. Refers generally to pressure waves associated with chemical reactions (and associated heat). Typical examples on nuclear power plants include hydrogen explosions, oil mist explosions and dust explosions. High Energy Arcing Faults (HEAF) are also generally included under this category.
Flooding	Considers releases of large quantities of liquids (usually water) from vessels or pipework. Spray onto sensitive electronic equipment is also usually considered in this context. The internal flooding hazards currently identified on site are those associated with water tank and pipe bursts.
Pipe Whip	Refers to a failure and subsequent release of potential energy in pressurised pipe work. This hazard is characterised both by the impact of the whipping pipe and the fluid jet which accelerates the pipe. The jet force is usually considered to be equal and opposite to the whipping force.
Steam Release	Considers over pressurisation and high temperature effects due to failure of steam pipes or superheated water.
Missile	The missile hazard can be broadly split into three categories, generated by: • Rotating machines (excluding main steam turbine) • Main steam turbine/generator • Failure of pipe work or vessels The main steam turbine type missile is usually considered separately as the velocities and energies involved are usually much greater than other missiles on site.
Blast	Refers generally to pressure waves associated with failure of pressurised equipment (pipe work and vessels). A list of typical internal blast hazard sources is: • Pressurised reactor systems • Non-combustible gas cylinders (e.g., oxygen) • Liquefied storage tanks
Electromagnetic Interference (EMI)	EMI is considered for equipment which can generate an electromagnetic field and its impact of other plant equipment. The assessment of EMI usually covers Radio Frequency Interference (RFI).
Dropped Loads	Considers impacts on plant and buildings civil structure due to the failure of lifting / mechanical handling equipment. Toppled, swing and collapsed

Individual Hazard	Definition
	loads (due to unplanned crane movements, crane failures or local support failures) are also usually considered as part of this topic.
Hazardous Materials	Assessment of toxic, corrosive or asphyxiant materials on plant equipment and personnel. This hazard requires some knowledge of items which are usually plant specific. A list of typical hazardous materials is: • Gas cylinders (e.g., nitrogen) • Atmospheric storge tanks (e.g., hydrazine hydrate) • Batteries (e.g., sulphuric acid)
Vehicular Transport Impact	Assessment of vehicle impact hazards on plant equipment or structures. This hazard requires some knowledge of items which are usually plant specific.

15.7.2.2 Combinations of Hazards

In addition to hazards occurring as single events, some event sequences or equipment failures can lead to situations where SSC are challenged by multiple or "combined" hazards. Internal hazards combinations are categorised into three groups:

Consequential Hazards: combinations where the primary hazard initiates a secondary hazard i.e., the cause of the secondary hazard is the primary hazard.

Correlated Hazards: combinations of hazards where more than one type of hazard is initiated by the same underlying cause.

Independent Hazards: combinations where there is no causal relationship between the hazard initiators. These types of combinations will only be considered for assessment if the individual hazard frequencies sum to give an overall frequency of >1.0E-07 /yr.

The Internal Combined Hazards Methodology and Identification Report [118] highlights the approach to combined hazards and the method for identifying and screening combined hazards. The methodology provides a screening table for each of the blocks in Reactor Island to identify the potential combinations of correlated hazards.

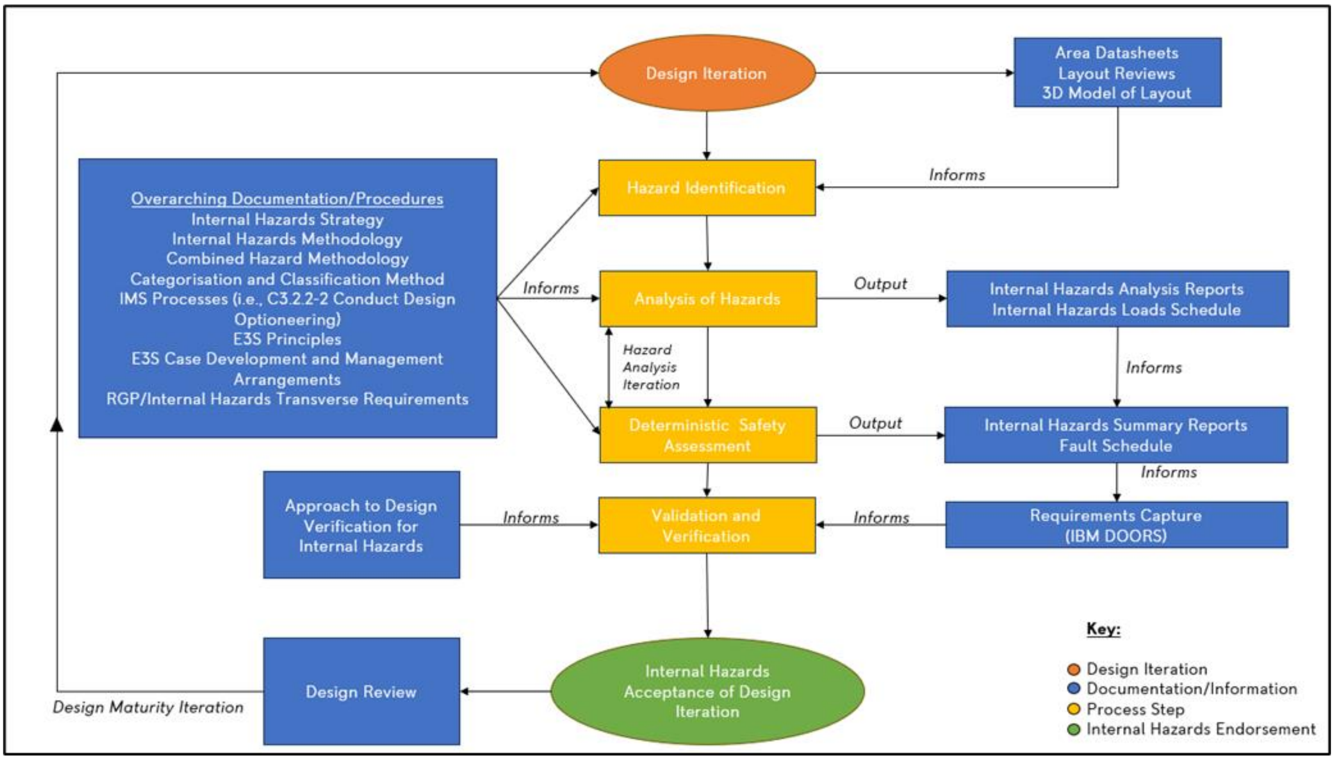
This chapter is based on a reference design prior to DRP1 (RD6) and as such, identifies potential combinations of correlated hazards within Reactor Island only due to the level of maturity available at the time of writing the report. Combined hazards outside of Reactor Island are addressed in the Internal Hazards Summary Report – Outside Hazard Shield [117], which is based on DRP1.

The RR SMR will also demonstrate plant resilience to external-internal hazard combinations. External-internal hazard combinations have not yet been identified; the Internal/ External Combined Hazards Report will be conducted in GDA Step 3, based on DRP2 and included in Version 3 of the RR SMR E3S Case.

15.7.3 Approach

This section details the internal hazards process. The approach to internal hazards analysis is shown in **Figure 15.7-1**.

Figure 15.7-1: Internal Hazards Processes



15.7.3.1 Internal Hazard Layout Reviews

During design iteration, Internal Hazards Layout Reviews have been conducted to ensure the layout is optimised to eliminate or minimise the impact of internal hazards. These reviews provide an early opportunity to optimise the layout with respect to internal hazards and initiate layout iteration on the back of any feedback provided by the Internal Hazards Team.

The Internal Hazard Layout Reviews provide identification and qualitative assessment of key hazards within an area using the following steps:

1. Identification of Key Hazards

2. Define Unmitigated Hazard Effects

3. Identify Options for Protection

4. Identify Actions where required e.g. confirm unknown information, consider an aspect in further detail outside of the meeting, or a specific requirement to update the design.

Hazard Protection Tables are produced to capture the findings of the Internal Hazard Layout Reviews, which will comprise the points above. Actions captured from the meeting will be monitored until closure.

This stage of the process is iterative. Any subsequent layout changes need to be revisited by the Internal Hazards Team. As the design develops, the scope and depth of the reviews increase relative to the level of detail available.

More information on Internal Hazard Layout Reviews is provided in the Internal Hazards Strategy [113].

15.7.3.2 Hazard Identification

Hazard identification for Internal Hazards is achieved via Area Datasheets, which are automatically updated against the design using the RR SMR requirements database. The format of the Area Datasheets is such that all the required parameters are provided for every equipment item, making it possible to search the Area Datasheets for the purpose of hazard identification.

The Area Datasheets is a module within the requirements database which is populated automatically by using the Functional Bill of Materials (FBOM) module and the Locations Register module. The FBOM presents a list of operating equipment that forms part of a system along with the various design parameters associated with each item of operating equipment e.g. pressure and temperature. The Locations Register module stores the layout information for each item of operating equipment e.g. the Reactor Island Block, Train etc.

Hazard Identification and screening for individual and combinations of all key hazards has been undertaken for each plant area, and a group of hazards have been identified for a particular area and a bounding hazard case defined and assessed (considering multiple / consequential hazards where applicable).

Hazard sequences have been grouped based on the challenges to specific targets, such as hazard barriers, SSCs performing safety functions, or VHR equipment. The physical withstand of these targets are then defined in relation to the worst-case combination of hazards to which they are subjected. The combined hazard loading is bounding through the design process (noting that the loading will be refined as the plant geometry and layout are developed, and as the detailed modelling of hazards is completed).

The Area Datasheets for Reactor Island (within Hazard Shield) are captured in [119]. Note, Area Datasheets are not available for Outside Hazard Shield at the present time due to low design maturity.

15.7.3.3 Analysis of Internal Hazards

The hazards identified in the relevant areas of the RR SMR have been analysed by applying the Internal Hazards Methodology [115]. This involves detailed analysis (where maturity is available) on the sources of internal hazards within the relevant layout areas. The result of this analysis is reported in the two main summary reports:

- Internal Hazards Summary Report -Within Hazard Shield [116]
- Internal Hazards Summary Report – Outside Hazard Shield [117]

The summary reports are split to summarise the internal hazards analysis inside and outside of the Hazard Shield. This is because the internal hazards postulated within the Hazard Shield impact nuclear safety systems while the internal hazards postulated outside the Hazard Shield affect the integrity of the hazard shield and radiological waste buildings.

The results of the analysis are also used indicatively by the design teams for specific system studies. For example, indicative blast loadings have been provided to the design teams of the Accumulators to support a study into the potential resizing of the component.

Internal Hazards Analysis is further discussed in section 15.7.4.

15.7.3.4 Interfaces with Safety Assessment

The internal hazards analysis has been used to inform DSA, discussed in Section 5 of the Internal Hazards Methodology [115]. The DSA is described in section 15.5 above. The steps below show how DSA is applied to Internal Hazards:

1. Define PIE
2. Identify required safety measures
3. Characterise hazard and define effects on safety measures
4. Identify hazard protection
5. Classify hazard protection and define performance requirements
6. Record and substantiate hazard protection

The Internal Hazards PIEs are captured in the Definition of PIEs and Derivation of Initiating Event Frequencies report [17] as well as in Appendix B (section 15.12). The report defines the PIEs and highlights the applicable operating modes and the IEF of the PIEs. The identified PIEs have been fed into the Fault Schedule report [19] where the E3S requirements on safety measures are presented. The fault schedule captures safety categorised functional requirements on the safety measures to ensure tolerance to internal hazards. The RR SMR requirements management database is used to manage the requirements flow and ensure that SSCs are designed against those requirements. Further information regarding DSA is captured above in section 15.5.

In addition to DSA, which is the primary focus for internal hazards, there will also be an internal hazards PSA and SAA carried out which will influence the design for internal hazards.

PSA is discussed in section 15.6. Initial hazards PSA is being conducted in GDA Step 3 (based on DRP2) to determine bounding assessments for hazards.

Internal hazards will also have an interface with SAA as internal hazards have the potential to initiate severe accidents and compromise the ability of claimed systems to respond during the management of the accident. SAA is discussed in section 0.

15.7.3.5 Validation and Verification

The verification process is discussed in E3S Case Tier 1 Chapter 3 Safety Objectives & Design Rules for SSCs [11]. Evidence of verification for specific systems is provided in the corresponding E3S Case Tier 1 Chapter for the system it is applicable to. For example, evidence of verification of Civil

Engineering Works & Structures is found in E3S Case Tier 1 Chapter 9B: Civil Engineering Works & Structures [120].

Following the DSA process outlined in 15.7.3.4, the internal hazards analysis is then subject to Validation and Verification. This process is informed by the Approach to Design Verification for Internal Hazards [121]. The methods used for the analysis of the individual internal hazards are validated using this approach.

Following Validation and Verification, a DR is carried out to confirm that the layout iteration is tolerant to internal hazards.

The Approach to Design Verification for Internal Hazards [121] document is the strategy to verify that an SSC design meets internal hazards requirements. The document details the methods of analysis, physical and simulated. The document also details the verification approach for the different internal hazards explored in the report, including the functional verification and transverse verification aspects for each hazard. The verification evidence will be captured in the RR SMR requirements management database.

15.7.3.6 Transverse Requirements Capture/ Relevant Good Practice

The approach to internal hazards analysis in the RR SMR incorporates RGP as overarching information. RGP has been used to develop the strategy [113] and methodology [115] documents which have been used to inform the internal hazards process (see **Figure 15.7-1**).

Internal hazards requirements are used to inform the design, these are safety categorised functional requirements and non-functional system (transverse) requirements. These are defined in Chapter 1 [3].

The internal hazards transverse requirements were developed by consulting RGP, such as Protection against Internal Hazards in the Design of Nuclear Power Plants (IAEA Safety Standards Series No. SSG-64) [122]. A Gate Review (GR) process was undertaken to identify key stakeholders (such as layout, civil engineering and build certainty) and workshops were carried out to ensure the requirements developed were relevant and feasible. The output of this process is captured in [123].

15.7.4 Internal Hazards Analysis

This section summarises the analysis for each of the individual hazards captured in Table 15.7-1 for both inside and outside hazard shield.

The hazard sources that are identified in the Reactor Island within the Hazard Shield are analysed in the Internal Hazards Analysis – Reactor Island within Hazard Shield report [124] and the Internal Hazards Fire Analysis Report [125]. The results of the analysis have been presented in the report and inform the Internal Hazards Summary Report – Within Hazard Shield [116]. Due to the level of design maturity, the analysis varies depending on the hazard.

The hazard sources that are identified outside of the hazard shield are analysed in the Internal Hazards Analysis – Outside Hazard shield report [126]. The results of the analysis are presented in the report and this is used to inform the Internal Hazards Summary Report – Outside Hazard Shield [117]. The level of design maturity in the areas outside of the hazard shield is lower than the maturity of the areas within the hazard Shield.

15.7.4.1 Fire

Modelling fire effects in specific blocks within Reactor Island is not considered to be practical at the level of maturity available at the design reference prior to DRP1, as there is not enough detail in the layout to provide sufficient inputs to the fire modelling.

Fire analysis has instead been carried out on typical sized compartments to be used in the RR SMR using the decoupling load of 4 hours against the BS 476 temperature-time standard fire curve. The compartments considered are a larger compartment (Process Room) and a smaller compartment (Electrical Room). The results of the fire modelling for the compartments have been reported in the Internal Hazards Fire Analysis Report [125].

The Fire Analysis Report [125] details the approach to fire modelling as well as describing the modelling software and the initial inputs to the modelling tool. Consolidated Model of Fire Growth and Smoke Transport (CFAST) is the tool selected to model the effects of the various compartment fires. The input information used for the analysis included the thermal properties, compartment geometry, ventilation and number and fraction of surface connections.

Modelling of different scenarios resulted in a number of general outcomes as well as specific output parameters such as maximum temperature, output combustible loads and output energy density. The outputs generated have been used to assess the design of the compartments against BS 476. This information has been used to inform the DRP1 layout contributing to a more tolerant design with regards to internal fire. Based on the maturity of the layout, indicative decoupling loads have been defined for fire and the civil barriers and structures will be substantiated against these loads.

The Internal Hazards Summary Report – Outside Hazard Shield [117] identifies the three main sources of fire outside of the hazard shield which are the High Voltage Essential AC Standby Generation System (BDV) Diesel Storage, Hydrogen and Hydrazine storage and the Main Transmission Area. The distance from hazard shield to the main transmission area is large enough that a fire in this area is bounded by the other fire cases outside of hazard shield.

Fire analysis for these areas has been presented in the Internal Hazards Analysis – Outside Hazard Shield [126] report and models both a diesel fire in the diesel storage building (using DRP1 dimensions) and a flammable gas fire resulting from the rupture of a hydrogen cylinder and a trailer storing 10 hydrogen cylinders.

The diesel fire analysis has been used to indicate the radiative heat flux on the hazard shield and Auxiliary Block Structure. The analysis is split into two cases, where the diesel is confined to the back-up generation building (Case 1) and where the diesel is confined to the bund (Case 2). The maximum surface temperature of the fire and its duration of the fires in both cases have been identified in the analysis. These parameters have been used to show that the identified cases do not threaten the Auxiliary Block or Hazard Shield Structure.

The hydrogen fire analysis has been used to determine a worst-case scenario which could impact target buildings. This has been identified as a 50 mm leak from one cylinder and one trailer (ten cylinders). This has allowed potential mitigation measures to be identified as shown in the analysis report.

15.7.4.2 Explosion

Explosion analysis is carried out for a number of different explosion types, including flammable gas, oil mist and HEAF. Within the Internal Hazards Analysis – Reactor Island within Hazard Shield [124] report, the flammable gas hazards within the Hazard Shield are characterised, the flammable cloud size determined and the explosion is modelled. Input information for oil mist hazards is based on a generic case informed by RGP [124] as the specific locations of oil mist sources are not yet defined. Using these parameters, the overall overpressure in the room can be calculated. For HEAF, input information is also limited and so assumptions have been made on a generic case. The HEAF analysis includes characterisation of HEAF hazards, determination of arc energy and equivalent of TNT (trinitrotoluene) and evaluation of barrier response.

The Internal Hazards Analysis – Outside Hazard Shield [126] has modelled hydrogen explosions from the failure of a single hydrogen cylinder and a trailer of hydrogen cylinders (ten cylinders) to provide blast overpressures at various radii from the blast source. The outputs of these calculations are compared to the structural damage criteria of reinforced concrete [127] as well as the generic site criteria for maximum overpressure on a flat wall.

15.7.4.3 Flooding

Flooding analysis is carried out following an iterative approach using equations presented in the Internal Hazards Methodology [115]. For blocks that contain flooding sources and require analysis, a number of assumptions are made before assessing the various cases in the blocks. Examples of the assumptions include location of the pipe break causing the flood and the diagnosis time.

Relevant inputs to the analysis inside the Hazard Shield (such as tank volumes and pump flow rates) are identified in the Internal Hazards Analysis – Reactor Island within Hazard Shield report [124] and values for maximum volume, maximum flood height, time to maximum flood height and duration of flood are calculated and presented for each of the cases.

The results are used to determine which of the safety systems within the blocks affected by flooding. The Internal Hazards Summary Report –Reactor Island within Hazard [116] summarises the analysis for each of the relevant blocks in Reactor Island.

The Internal Hazards Summary Report – Outside Hazard Shield [117] identifies the sources of flooding outside of the hazard shield. The maturity of this analysis is low and as such, high level identification of bounding cases has been carried out. The bounding case identified is that several water tanks with volumes up to 1500 m^3 are distributed around site. Failure of one or more of these tanks could result in the drainage capacity of the site becoming overwhelmed. Using this bounding case, it has been recommended that the SSCs are situated above the internal flood level to prevent ingress of water and damage to the SSCs.

15.7.4.4 Pipe Whip

Pipe whip analysis has been carried out by using the system information found in the Area Datasheets and specific dimensions of pipework (from pipe schedule) in accordance with the internal hazards methodology [115] to determine parameters such as the reaction force, whipping length, impacting energy and impacting velocity.

The Internal Hazards Analysis – Reactor Island within Hazard Shield report [124] includes the equations to be used for calculating pipe whip effects and the origin of the equations is noted in the internal hazards methodology. Bounding cases have been identified within the relevant blocks to determine the most onerous cases of pipe whip. The Internal Hazards Summary Report – Reactor Island within Hazard Shield [116] summarises the pipe whip analysis for each of the relevant blocks within Reactor Island.

Pipe whip sources outside of the Hazard Shield have been identified in the Internal Hazards Summary Report – Outside Hazard Shield [117]. The report shows the main sources of pipe whip and details the case parameters used to determine a bounding case. The case identifies values for maximum pipe length and maximum impacting energy to be factored into design decisions.

15.7.4.5 Missiles

Missiles in the RR SMR can originate from pressure part failure of vessels and high-pressure valves and failure of rotating machinery. Missile analysis is carried out by identifying the type of missile source present in the area.

Missiles within Reactor Island are identified and analysed in the Internal Hazards Analysis – Reactor Island within Hazard Shield report [124] and are summarised for each block within Reactor Island in the Internal Hazards Summary Report – Reactor Island within Hazard Shield [116].

Missiles outside of the Hazard Shield are identified and analysed in the Internal Hazards Analysis – Outside of Hazard Shield [126] report and are summarised for the areas outside the Hazard Shield in the Internal Hazards Summary Report – Outside Hazard Shield [117].

For pressure part failure missile analysis, input information including the vessel dimensions, pressure and temperature, is used to determine the energy, velocity and range of the missile.

For rotating machinery missiles, potential sources are identified and where specific information about the source information is available, specified values for impeller dimensions and angular speeds have been used. Where this is not possible, an assumed value for the parameters has been used. This information is used to calculate the velocity and kinetic energy of the missile fragments.

15.7.4.6 Blast

Blast analysis is conducted similarly to the pressure part failure missiles analysis. The inputs into the analysis include vessel dimensions, pressure and temperature which can be found using the Area Datasheets. This information is used to determine the target distance, scaled stand-off distance, peak side-on overpressure, positive side-on impulse and impulse time.

Blast calculations and results for sources within Reactor Island are captured in the Internal Hazards Analysis – Reactor Island within Hazard Shield report [124] and the sources and results of these calculations are summarised in the Internal Hazards Summary Report – Reactor Island within Hazard Shield [116].

Blast calculations and results for sources outside of Reactor Island are captured in the Internal Hazards Analysis – Outside Hazard Shield report [126] and the sources and results of these calculations are summarised in the Internal Hazards Summary Report – Outside of Hazard Shield [117].

15.7.4.7 Hazardous Materials

Hazardous materials have been mainly considered as part of the outside hazard shield internal hazards analysis. This is due to the more onerous cases of hazardous materials being found in these areas. There are cases within Reactor Island that have been considered as part of the Internal Hazards Analysis – Reactor Island within Hazard Shield report [124] and summarised for each block in the Internal Hazards Summary Report – Reactor Island within Hazard Shield [116].

The analysis of hazardous materials outside of the Hazard Shield is carried out in the Internal Hazards Analysis – Outside Hazard Shield [126] report. The outputs are summarised in the Internal Hazards Summary Report – Outside Hazard Shield [117].

The analysis uses the industry standard Phast modelling tool to model bounding toxic and asphyxiation scenarios. The analysis has given confidence to design engineers that within the site-specific layout there is scope for toxic gases to be located at a safe distance from nuclear safety significant buildings. As maturity increases, further assessment of hazardous materials will take place when inventory and physical stage of storage gases is defined.

15.7.4.8 Vehicular Transport Accidents (VTA)

As for hazardous materials, the more onerous cases of VTA are found outside of the Hazard Shield. The cases within the Hazard Shield are identified and analysed in the Internal Hazards Analysis – Reactor Island within Hazard Shield report and summarised for each block in the Internal Hazards Summary Report – Reactor Island within Hazard Shield [116]. The cases outside the Hazard Shield are identified and analysed in the Internal Hazards Analysis – Outside Hazard Shield report [126] and summarised for each area in the Internal Hazards Summary Report Outside Hazard Shield [117]. A bounding case for segregated areas has been developed around the vehicles within the safety fluids block. The case defines the impact energies of the vehicles within the safety fluids block as this block will have the most onerous requirement for vehicles.

The Internal Hazards Summary Report – Outside Hazard Shield [117] highlights several sources of VTA outside the Hazard Shield. The report identifies the sources of VTA and determines a conservative bounding case. The layout of the berm, roadways and position of buildings is expected to restrict a vehicle reaching close to {REDACTED} and therefore more analysis will be carried out for VTA when the layout is more defined.

15.7.4.9 Summary of Internal Hazards Analysis

In summary, the internal hazards analysis has informed the design of the RR SMR, ensuring that measures to prevent and protect against internal hazards are identified and implemented. Based on the inputs, assumptions and results of the analysis, the assessment derives requirements for the civil and modular design in all areas of plant, including segregation barriers where applicable.

15.7.5 Protection Against Internal Hazards

15.7.5.1 Layout Optimisation

The safety case for internal hazards is largely built upon segregation i.e. the physical separation of SSCs by distance or by means of some form of barrier. The segregation of SSCs ensures that individual losses of equipment can be tolerated within the safety case due to redundant equipment remaining available.

The Architectural and Layout Summary Report [114] describes the process for the Reactor Island Layout, including the hierarchy of Layout decisions, the systems engineering approach to layout design and the applicable engineering governance processes. That report is based on DRP1 and contains a section discussing internal hazards considerations and how internal hazards has been incorporated into the overall layout design.

The internal hazards section of the layout report shows that segregation and separation of safety systems is considered in the design and uses the segregation of the safety fluids and Electrical, Control & Instrumentation (EC&I) systems trains within Reactor Island as examples. The segregation of these systems allows the plant to carry out FSFs if one of the trains is disabled due to internal hazards.

The layout report also explains how the interspace is set out to mitigate the risk of steam release and pipe whip associated with the main steam and feed lines and to address the bounding blast case for Reactor Island (Accumulators). The layout report also demonstrates how the layout has been optimised to improve the tolerance to various internal hazards such as fire, missiles and VTA.

As the layout is progressed, the design shall be optimised through design iteration to reduce internal hazards risks to ALARP in each of the Reactor Island blocks. At DRP1, the tolerance to internal hazards is greatly improved in comparison to previous reference designs and will continue to improve through design iteration.

15.7.5.2 Segregation

Within the DRP1 layout, segregation of SSCs is largely achieved by distance and civil barriers. The various blocks are surrounded by a civil structural envelope and the systems within are segregated either by distance or further civil barriers (in the case of the accumulators in the Interspace).

The Modular Kit of Parts (MKoP) will be utilised where practicable to provide barriers between systems within trains. An example of where this is required is within the EC&I block due to the need to segregate diverse systems of C&I (RPS and DPS) within the same train.

The MKoP Primary Structure Standard Frame Design Definition document [128] contains a section demonstrating how tolerance to internal hazards has been incorporated in the modular design. The tolerance to internal hazards is demonstrated in this document by identifying the design criteria developed by the individual internal hazards requirements. This allows options to be identified for the protection against internal hazards. For example, options for protecting the metallic structure from fire including intumescent paint and barriers have been identified.

The MKoP Barriers Design Definition document [129] discusses the different barrier design solutions that have been generated to protect SSCs and the requirements on the solutions due to internal hazards. The internal hazards requirements are used as one of the design inputs for the barriers and are used to develop concepts for different barrier solutions such as fire walls, flood barriers and blast curtains.

15.7.5.3 Safety Measures

The Internal Hazards Entries to the Fault Schedule identifies the claims on the specific safety measures required in the event of an internal hazard. As described in the DSA section (15.5) above, the identified Internal Hazard PIEs (see Appendix B, section 15.12) and safety measures are included in the Fault Schedule [19]. The measures identified are categorised according to the RR SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method [86].

When an internal hazards PIE is inputted to the Fault Schedule, the principal safety measure (Category A) is identified as well as a diverse measure (Category B) and any other required safety measures such as failsafe and risk reduction measures (Category C). Category A, B and C safety measures are applied to each of the FSFs: CoFT, Control of Radioactive Materials (CoRM) and CoR. Note that the diverse measure may be initiated chronologically before the principal measure.

An example of the safety measure requirements is as follows; INT.1.1.01 (Fire in Containment) requires Auto SCRAM (category A), Alternative Shutdown Function, ASF, (Category B) and fire withstand/protection of DPS/RPS1 cables as the safety measures for CoR. This is captured in the Fault Schedule [19].

The safety categorised functional requirements derived from the internal hazards entries to the Fault Schedule [19] have been developed through a GR process to ensure that the requirements are realistic and achievable and that they are captured in the design process.

Through the development of the Fault Schedule, safety categorised functional requirements have been developed regarding VHR equipment. For example, Internal Hazards Requirement 1.10.1.0-8 states that “VHR equipment shall not experience structural integrity failure due to internal hazards”.

15.7.5.4 Verification and Validation

The Approach to Design Verification for Internal Hazards [121] document is the strategy to verify that an SSC design meets internal hazards requirements. The document details the methods of analysis, physical and simulated. The document also details the verification approach for the different internal hazards explored in the report, including the functional verification and transverse verification aspects for each hazard.

15.7.6 Outputs

The internal hazards analysis has informed the Fault Schedule [19] by identifying which internal hazards contribute to a PIE. Using the layout reviews and internal hazards analysis/summary reports, hazard sources have been identified by block and grouped according to the safety claims for each hazard.

A summary of the output requirements from the Fault Schedule is shown for each block in Table 15.7-2 below. A full description of the PIEs identified below is captured in the Definition of PIEs Report [17] and the full Fault Schedule entries are captured in the Fault Schedule [19].

Table 15.7-2: Internal Hazards Outputs from Fault Schedule

PIE	**Internal Hazards Contributing to PIE**	**Requirements**
	Containment	
Fire in Containment (INT.1.1.01)	Fire	Failsafe claim on control rods requires that rods drop into core if EC&I signal is lost due to fire. EC&I trains controlling FSFs shall have sufficient withstand to fire or protection shall be applied to divisions of EC&I cabling to prevent loss of multiple trains of safety systems. Pipework of systems providing FSFs shall have sufficient withstand to fire or protection shall be applied to divisions of pipework to prevent loss of multiple trains of safety systems.

PIE	Internal Hazards Contributing to PIE	Requirements
LOCA Conditions in Containment (INT.1.1.02)	Flood Steam Release	Failsafe claim on control rods requires that rods drop into core if water/steam leads to loss of electrical connection. EC&I trains controlling FSFs shall have sufficient withstand to water/steam or protection shall be applied to divisions of EC&I cabling to prevent loss of multiple trains of safety systems. Pipework of systems providing FSFs shall have sufficient withstand to water/steam or protection shall be applied to divisions of pipework to prevent loss of multiple trains of safety systems.
Minor Disruptive Pipe Failure in Containment (INT.1.1.03)	Pipe whip or Blast that does not reach a critical target.	Claim that ECC can provide cooling in relevant double-break LOCA scenarios. EC&I trains controlling FSFs shall be sufficiently separated/segregated to prevent loss of multiple EC&I trains due to disruptive pipe failure. HPIS pipework shall be sufficiently separated/segregated to prevent loss of redundant HPIS trains. Passive Core Cooling System (PCCS) heat exchangers shall be sufficiently separated/segregated to prevent loss of redundant PCCS trains.
Restrained Pipe Whip in Containment (INT.1.1.04)	Large bore pipe hits intermediate bore pipe. Intermediate bore pipe hits another intermediate bore pipe.	Claim that ECC can provide cooling in relevant double-break LOCA scenarios. EC&I trains controlling FSFs shall be sufficiently separated/segregated to prevent loss of multiple EC&I trains due to disruptive pipe failure. HPIS pipework shall be sufficiently separated/segregated to prevent loss of redundant HPIS trains. PCCS heat exchangers shall be sufficiently separated/segregated to prevent loss of redundant PCCS trains.
Blast or Catastrophic Pipe Whip in Containment (INT.1.1.05)	Pressuriser or SG blast, double intermediate bore LOCA, MSLB plus LOCA.	ECC cannot protect against the contributing internal hazards. The pressuriser, SG, and large bore pipework in containment must be classified as VHR.

PIE	Internal Hazards Contributing to PIE	Requirements
RCP Disintegration (INT.1.1.06)	Rotating Machinery Missiles.	RCP Casing must contain any missiles generated by the RCP.
Valve Stem Missiles (INT.1.1.07)	Pressure Part Failure Missiles.	Valves must be orientated such that the direction of the generated missiles avoids damaging multiple trains of safety systems.
Interspace		
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Fire in the Interspace (INT.1.2.01)	Fire	Safety blocks/trains (safety EC&I, safety fluids, fuelling block) shall be protected from fire in the interspace by external envelope of the block/train. LUHS, Accumulators, ASD valves/lines, SGRVs/lines shall be suitably separated/segregated to prevent loss of multiple safety systems due to fire.
Steam/Flood in Interspace/Inside Hazard Shield (INT.1.2.02)	Steam Release Flood	Steam released within the Interspace shall not reach safety blocks/trains (safety EC&I, safety fluids, fuelling block). Flooding and steam release shall not affect the serviceability of the MSIVs or the Feed Isolation Valves
Accumulator Failure (INT.1.2.03)	Blast Missiles	Safety blocks/trains (safety EC&I, safety fluids, fuelling block) shall be protected from accumulator blast by internal civil barriers (accumulators within buttresses). Redundant accumulators and LUHS tanks to be segregated by both civil barriers and distance (located in opposite corners or interspace).
Main steam line Pipe Whip/Missiles (INT.1.2.04)	Blast Missiles Pipe Whip	Safety blocks/trains (safety EC&I, safety fluids, fuelling block) shall be protected from MSLB by the external envelope of the safety blocks. Redundant lines of main steam line shall be segregated (SCRAM can provide protection from singular MSLB but not double or triple)
Other Infrequent Hazards Originating in the Interspace (INT.1.2.05)	Explosion Blast (non-MSL) Missiles (non-MSL) Pipe Whip (non-MSL)	Safety trains shall be segregated to prevent loss of multiple trains due to infrequent internal hazards in the interspace.

PIE	Internal Hazards Contributing to PIE	Requirements
	Hazardous Materials Release Vehicular Transport Accident	
	Safety Fluids Block	
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Fire in Safety Fluids Block (INT.1.4.01)	Fire	Other Reactor Island Blocks (Containment, Safety EC&I Block/Trains, Fuelling Block and Interspace) shall not be affected by fire in the Safety Fluids Block. Redundant trains of ASF, HPIS, Chemistry and Volume Control System (CVCS), LUHS and CSCS shall be suitably segregated to prevent loss of multiple trains of safety systems due to fire.
Flooding in Safety Fluids Block (INT.1.4.02)	Flooding	Other Reactor Island Blocks (Containment, Safety EC&I Block/Trains, Fuelling Block and Interspace) shall not be affected by flooding in the Safety Fluids Block. Redundant trains of ASF, HPIS, CVCS, LUHS and CSCS shall be suitably segregated to prevent loss of multiple trains of safety systems due to flooding. Appropriate drainage routes shall be in place to remove standing water to a relevant sump/tank.
Other Infrequent Hazard in Safety Fluids Block (INT.1.4.03)	Pipe Whip Blast Explosion Missile Hazardous Material Release Vehicular Transport Accident	Other Reactor Island Blocks (Containment, Safety EC&I Block/Trains, Fuelling Block and Interspace) shall not be affected by infrequent internal hazards in the Safety Fluids Block. Redundant trains of ASF, HPIS, CVCS, LUHS and CSCS shall be suitably segregated to prevent loss of multiple trains of safety systems due to flooding.
	Safety EC&I Block	
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Internal Hazard in Safety EC&I Block	Fire Flooding	Internal hazards in the Safety EC&I block/trains shall not spread to other blocks in Reactor

PIE	Internal Hazards Contributing to PIE	Requirements
(INT.1.5.01)	Explosion Pipe Whip Blast Missile Hazardous Material Release	Island (Containment, Safety Fluids Block, Fuelling Block and Interspace). Internal hazards in the Safety EC&I block/trains shall not affect LUHS and accumulators. Redundant trains of EC&I systems shall be suitably segregated to prevent loss of multiple trains of EC&I.
Fuelling Block		
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Fire in the Fuelling Block (INT.1.3.01)	Fire	Design of the Fuel Pool Cooling System (FPCS) shall be hazard resistant.
Flooding in the Fuelling Block (INT.1.3.02)	Flooding	Design of the FPCS shall be hazard resistant.
Other Infrequent Hazard in the Fuelling Block (INT.1.3.03)	Explosion Missiles Vehicular Transport Accident	Design of the FPCS shall be hazard resistant.
Auxiliary Block		
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Internal Hazard in the Auxiliary Block (INT.1.5.01)	Fire Flooding Explosion Blast Pipe Whip Missiles Hazardous Materials Release Vehicular Transport Accident	System design shall be hazard resistant. Waste storage and waste processing systems shall be segregated by barriers
Main Control Room		
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Internal Hazard in the Main Control Room (MCR)	Fire Flood Explosion	Redundant Safety EC&I trains shall be segregated from the MCR to prevent loss of multiple trains of EC&I.

PIE	Internal Hazards Contributing to PIE	Requirements
		The Supplementary Control Room (SCR) shall be suitably segregated from the MCR and shall have capacity for monitoring reactivity. LUHS and accumulators shall not be affected by internal hazards in the MCR. ECC and IVR shall be monitored by SCR.
Outside the Hazard Shield		
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
Turbine Disintegration	Turbine Missiles	Standby Alternating Current Diesel Generators, Reactor Island, SGRVs and emergency centres shall be located outside of missile cone.
Other Internal Hazards Outside the Hazard Shield	Fire Explosion Flooding Hazardous Material Release Missile Blast Steam Release Vehicular Transport Accident	Redundant trains of standby generators shall be suitably segregated to prevent loss of back-up AC power.
General		
PIE	**Internal Hazards Contributing to PIE**	**Requirements**
EMI	EMI	Loss of trains due to EMI shall be limited to a maximum of one train of EC&I, Safety Fluids and Back-up Diesel Generation
Hazardous Materials Affecting MCR Habitability	Hazardous Material Release	SCR shall have capacity to monitor all FSFs. SCR HVAC shall be separate to MCR HVAC.

15.8 External Hazards Analysis

15.8.1 Overview

In addition to plant faults, RR SMR considers external hazards in the context of nuclear safety, i.e., hazards arising from outside the site boundary of the power station that are considered as PIEs that could challenge the delivery of the FSFs. External hazards are defined by the ONR as 'natural or man-made hazards to a site and facilities that originate externally to both the site and its processes' [130].

At RD7/DRP1, focus has been on the development of an appropriate and justified list of external hazards for the RR SMR, which is presented in this section with the relevant screening criteria that has been applied.

Furthermore, E3S Case Tier 1 Chapter 2: Generic Site Characteristics [131] outlines the set of parameters and conditions that are derived for each external hazard remaining after screening. This provides a bounding GSE that informs the design of the RR SMR, such that the design is capable of being built and operated in a way that is safe, secure, and tolerant to external hazards in GB.

15.8.2 List of External Hazards

15.8.2.1 Development Process

A complete list of potential external hazards for RR SMR was first produced in [132], based on a review of internal sources, RGP, United Kingdom (UK) Regulatory Guidance and international documentation including:

- RR SMR Hazard Log, [133]
- ONR Guidance:
  - ONR SAPs, [130]
  - ONR TAG 13, [134][12]
- WENRA guidance on new Nuclear Power Plant Design, [135]
- US NRC guidance on external hazards and PSA, [136] and [137].

A secondary review was carried out in [138], which examined the following additional guidance:

- Requirements produced by the EUR Organisation for new large and mid-sized Nuclear Power Plants, [37]
- Swedish Nuclear Inspectorate (SKI) Guidance on external hazards, [139]
- European Commission guidance on external hazards, [140]

[12] It is noted that a newer version of TAG 13 was released in October 2023 [149], this will be considered in GDA Step 3.

- Organisation for Economic Co-operation and Development (OECD) guidance on external hazards, [141]

- IAEA Safety Standard NS-G-1.5, [9]

As part of the development of the GB GSE, a further review of previous GDA submissions from other Requesting Parties (RPs) has been undertaken, to produce a final list of unscreened hazards, presented in [142].

15.8.2.2 Screening Criteria

The superset of unscreened hazards has been screened to those relevant to the RR SMR using the following criteria, which is developed from the SAPs [130]:

- Very low frequency of occurrence, for discrete hazards at a GB site this is less than 1E-07 /yr.

- Low potential consequences from associated fault sequences if they are incapable of posing a significant threat to nuclear safety.

Additionally, several hazards are screened in for consideration. However, they are judged to be site specific; [134] and [143] recognise that it is difficult to develop some external hazards that are site specific as part of GDA. For example, consideration of the coastal flood hazard is not possible until a site has been selected; however, RR SMR currently assumes the ‘dry site concept’, as discussed in [8]. Further guidance is given in [143] which states that the definition of the site envelope can be as broad or narrow as the requesting party wishes. The GB GSE [142] has divided the screened hazards into the following categories [143]:

- Within scope of GDA.

- Site-specific but reassurance has been provided during GDA.

- Site-specific and only able to be treated as such in any detail.

15.8.2.3 External Hazard List

The values for external hazards are determined following the approach outlined in ONR SAPs (text repeated below from [130]):

For man-made external hazards the design basis is defined in one of two ways:

- Probabilistically, as a best estimate value of hazard severity and frequency of occurrence down to about 1E-05/yr (FA.5, paragraph 628(a) [130]), or;

- Deterministically, as a maximum credible event (paragraph 242 of [130]).

For natural external hazards defined by hazard curves, the design basis is defined as follows:

- Probabilistically, as a conservative estimate of hazard severity at the 1E-04/yr frequency of exceedance point on the hazard curve (EHA.4, FA.5 paragraph 628(c) [130]).

The list of external hazards that have been screened for the generic RR SMR design are outlined in Table 15.8-1, with a definition, and proposed mitigations noting these are not comprehensive and will change as the design evolves. Further mitigations are outlined in Section 15.8.4.

Any external hazards not included within issue 2 of the GB GSE will be incorporated into the up issued GSE in Step 3, for example, Loss of Offsite Water (LOOW).

There are also several external hazards that have site specific elements, for which the GSE provides commentary [142], summarised in Table 15.8-2.

Table 15.8-1: Screened in External Hazards

External Hazard	**Definition** [144], [145]	**Proposed Mitigations (TBC as the design matures)**
Air Temperature	A measure of how warm or cold the air is. Air temperature can be considered in terms of dry bulb and wet bulb temperatures, the former is the temperature of the air measured using a thermometer, the latter is the air temperature at 100 % relative humidity (noting the dry bulb and wet bulb air temperatures would be identical at 100 % relative humidity, otherwise the wet air temperature is always lower). For the RR SMR design, the ESWS and MCWS have cooling towers which are susceptible to wet bulb air temperatures, HVAC chillers are susceptible to dry bulb air temperatures. In general, if not appropriately cooled, C&I, electrical equipment and other SSCs may be vulnerable to air temperature if rooms reach temperatures outside of operating limits	HVAC
Relative Humidity	A measure of the relative saturation/moisture of the atmosphere.	HVAC
Wind	Steadily moving stream of air. The speed and direction of this stream of air can change over time. Missiles generated by wind (wind-induced missiles and wind-blown debris) are also considered.	Hazard Shield, redundancy & separation
Tornado	Localised and intense rotating low pressure vortex structures. Missiles generated by a tornado (tornadic missiles) are also considered.	Hazard Shield, redundancy & separation
Rainfall	Precipitation arriving at the surface in liquid form.	Hazard Shield, redundancy & separation
Hail, Snow and Sleet	The freezing of precipitation in the atmosphere.	Hazard Shield, redundancy & separation
Ice	Frozen water. The different types of ice considered and defined in the GSE are frazil ice, rime ice, clear ice and glaze ice [142].	Hazard Shield, redundancy & separation
Cooling Water Temperature	The temperature of the water used to provide cooling to the plant.	Back-up cooling water supplies Monitoring of cooling water temperature.
Lightning	A visible discharge of electricity.	Lightning Protection System
LOOP	The loss of available power to the plant from the off-site power supply network.	Diesel Generators
LOOW	The loss of available cooling water from off-site water sources.	ECC system

Table 15.8-2: Site Specific External Hazards

External Hazard	**Definition** [145], [146], [147], [148], [149]	**Proposed Mitigations (TBC as these hazards are site specific)** [114]
Seismic	The hazard relating to an earthquake. Primary seismic hazards are ground motion and surface fault rupture	Seismic Isolation System (Aseismic bearing)
Accidental Aircraft Crash	The accidental impact of an aircraft to the plant.	Hazard Shield, redundancy & separation
Landscape Changes	The changes to the natural landscape over time through factors such as erosion, ground movement or glacial rebound.	Taken into consideration when siting and will be factored in the civil design
Space Weather	Hazards arising from changing environmental conditions in near-Earth space.	Hazard Shield, Hardening of relevant SSCs
EMI	Electromagnetic radiation emitted from an external source which can affect electrical equipment.	Hazard Shield, Hardening of relevant SSCs
Flooding	The inundation and submerging of a usually dry area with water. Flooding can be coastal (including tsunami), fluvial and pluvial.	Usually, will involve flood barriers and potentially sea defences if required
Drought	A lack of precipitation over an extended timescale which results in a reduction in groundwater and moisture content as well as ground shrinkage.	Backup water supplies and monitoring. The timescales over which drought is expected to occur are long enough to respond to the hazard.
Geological	Hazards associated with the sub-surface features and conditions of an area.	Taken into consideration when siting
Industrial Hazards	Hazards arising from adjacent permanent facilities or the movement of hazardous materials. Industrial Hazards include: • Toxic and Corrosive Materials • Manmade Explosions • Manmade Fire • Manmade Missiles • EMI/RFI	Hazard Shield for explosions, missiles, fire and EMI/RFI. For toxic and corrosive materials, detection systems on air intakes. Redundancy & separation will also be used. Mitigation measures will be considered when siting, based on the potential for this hazard
Biological Phenomena	The intake or infestation of animals or biological debris.	Filters on intake systems alongside regular maintenance

While the provision of complete information for site-specific hazards currently cannot be determined at this stage of the GDA, general comments providing reassurance on their assessment and mitigation, in addition to bounding values where practical have been provided in the GB GSE [142]. In addition, for those applicable screened in hazards, climate change values have been calculated using the UK Climate Projections 2018 (UKCP18) [150]; a climate analysis tool that forms part of the Met Office Hadley Centre Climate Programme. A full list of hazard values is located in the GB GSE and E3S Case Tier 1 Chapter 2: Generic Site Characteristics [131].

Identification and assessment of site-specific hazards shall be undertaken at the site licensing and permissioning stages by the future dutyholder/licensee/permit holder. Furthermore, a comparison of site-specific data against the GSE shall be undertaken to confirm whether justification of external hazards for the generic design remains suitably bounding for the specific site, or if further assessment is required. This is captured as Commitment C15.1:

- **Commitment on Future Dutyholder/Licensee/Permit Holder C15.1**: The future dutyholder/licensee/permit holder shall identify all site-specific external hazards and derive appropriate design basis values making allowances for climate change where applicable and provide a suitable safety justification once a site has been selected.

15.8.3 External Hazards Combinations

The External Combined Hazards Report [151] presents a review of credible external hazards and a detailed list of external hazard combinations judged to be credible within a generic site in GB. The report outlines information on the magnitude and severity of each hazard in combination i.e. where the hazards may occur simultaneously, provide superimposed loadings or increase vulnerabilities onto safety systems. Combinations of hazards should be identified and considered as part of a DBA, PSA and SAA. Internal and external hazard combinations and consideration of external combined hazards beyond the design basis are currently excluded but will be considered in Step 3 of GDA.

The report considers the following hazard combinations:

- Consequential (external) hazards: An external hazard that is the direct effect of a primary, correlated or secondary hazard. For example, an external fire may be a consequential hazard resulting from a lightning strike.

- Correlated (external) hazards: An external hazard that can occur simultaneously with another hazard because both are associated with a common physical process. For example, more than one hazard may arise from the same meteorological condition; a tropical cyclone may induce high winds, extreme rainfall and high waves.

- Independent (coincidental) hazards: Hazards which may affect the site simultaneously on a random basis as independent events. For example, earthquake and air temperature hazards. These hazards are not correlated through an underlying physical process or caused by a common hazard event.

The External Combined Hazards Report [151] details and applies a proposed methodology for determining combined hazards that the design should withstand. The output of the report are lists of credible external hazards, which are given in three distinct sets:

- Individual Hazards (i.e. those outlined in Table 15.8-1 and Table 15.8-2).

- Combined Hazard Scenarios: a set of combined external hazards which may be considered to act in combination around a common causal condition or factor.

- Other credible Hazard Combinations that do not fall into a combined hazard scenario but should be considered.

The external hazard combinations require judgement to be applied and the decisions made have been guided by other GDAs, guidance, and input from a purpose held workshop. Justifications have been documented in External Combined Hazards Report [151].

The External Combined Hazards Report [151] lists the individual hazards against the hazard scenarios and provides the magnitudes for each hazard as associated with a particular scenario. These are described as one of the following:

- Design Basis Hazard: A non-discrete hazard which could affect the site with an Annual Frequency of Exceedance (AFoE) up to 1E-04/yr. for natural hazards and 1E-05/yr. for manmade hazards, or a discrete hazard which the design considers based on site specific hazard characterisation findings.

- Operating Basis Hazard: A non-discrete hazard which could affect the site with a AfoE up to 1E-02/yr. This is the hazard that might be expected to occur during normal operation of the plant.

Independent hazards that were not included within a scenario and apply a superimposed load or effect on an SSC were also considered.

The screened in combined hazard scenarios, as outlined in the External Combined Hazards Report [151] are as follows:

- A – Cold Weather
- B – Hot Weather
- C – Storm (including coastal, fluvial flooding)
- D – Earthquake (including consequential hazards)
- E – Solar Activity
- F – Tornadic Storm
- G – Accidental Aircraft Impact (including consequential hazards)
- H – Industrial Accident and Fire.

The external combined hazards report will be periodically updated with increasing maturity in the design. At the site-specific stage, the combined hazards report will need to be reviewed to ensure its conclusions are still applicable to the chosen site.

Commitment on Future Dutyholder/Licensee/Permit Holder C15.2: The future dutyholder/licensee/permit holder shall identify all site-specific combined external hazards and provide a suitable safety justification.

15.8.4 Analysis of External Hazards

As the generic E3S Case is developed to meet its objective 'to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design' [3], further arguments and evidence to underpin the claim will be developed in line with the E3S Case Route Map [4] and reported in future revisions of the generic E3S Case. This broadly includes continued iterative E3S analysis and finalisation of E3S requirements including environment, security and safeguards, detailed design development of all SSCs, and verification and validation of E3S requirements. This strategy applies to the analysis of external hazards (and other disciplines) to support the demonstration of ALARP.

Comprehensive analysis or testing to demonstrate that no external hazard can impact the delivery of the FSFs, and risks are reduced to ALARP, will be undertaken as the design is developed and evidence is produced in line with the E3S Case Route Map [4].

Requirements to withstand external hazards loads will be flowed from the GSE to SSCs. The Verification process, discussed in Chapter 3, will define the approach of how SSC design's will be substantiated against these requirements, and produce evidence.

Analysis or testing will be used to provide substantiation evidence that SSCs meet external hazard load requirements derived from GSE values.

Analysis work to is expected to consist of:

- Implementation of the external hazard methodologies (see below).
- Substantiation of structures from external hazards using structural analysis against design basis external hazard values as stated in the GSE [142].
- Substantiation of systems and components from design basis external hazard values as stated in the GSE [142] via hazard impact analysis.

The latest position on Verification & Validation (V&V) claims relating to external hazards are outlined in Chapters 4 to 11 of the E3S Case, with further discussion on verification outlined in Chapter 3 of the E3S Case. At RD7/DRP1, the V&V evidence comprises strategies and some performance analysis, with much of the substantiation to come in future iterations of the E3S Case.

15.8.5 Methodologies

15.8.5.1 Space Weather Hazard Methodology [152]

This document presents a brief background to the nature of the space weather hazard including applicable codes and standards and a summary of space weather events, effects, and impacts. A high-level methodology for the characterisation, assessment and mitigation of the hazard is also provided. Components of the space weather hazard are:

- Geomagnetically induced currents.
- Ground level enhancement of solar energetic particles.
- Solar radio bursts.

- Ionospheric disturbance.

Each hazard is quantified in terms of the relevant external physical characteristics. Bounding levels are provided for UK latitudes. Many of the hazard risk factors, both physical and technological, are site-specific and will require full consideration at the site-specific stage.

A range of potential mitigations are identified that will need to be refined as the design develops and finalised at the site-specific stage.

15.8.5.2 Analysis of Background Accidental Aircraft Crash Frequency [153]

This report outlines the methodology that was applied to determine the frequency of accidental aircraft crashes in GB. The Byrne method [154] was applied to the calculation of background accidental aircraft crash rate assuming that the generic location of the site is more than five miles from an aerodrome and not in the vicinity of a published air route or extended flightpath associated with an aerodrome. Chaplin suggested three changes to the Byrne method [155], namely:

- Merger of below-airway and background crash rates.
- Merger of all the military crash zones outside the vicinity of an aerodrome (normal, transition and concentrated crash zones).
- Merger of civilian-operated ex-military jets into the small transport category.

These suggested changes were reviewed and only the first two were adopted as reasonable for application to this analysis. The merger of civilian-operated ex-military jets into the small transport category was rejected as these were reclassified into the military categories.

The Air Accidents Investigation Branch database [156], was used as the authoritative source of accidents to civilian aircraft. Several different rates of accidents were calculated for different time periods and an appropriately conservative values selected.

The effective target area was calculated conservatively. The mean accidental aircraft crash rate onto the critical area of a RR SMR site was considered to occur with a frequency of less than 1.2E-06 /yr.

Additional site-specific work will be necessary when a site for the RR SMR is confirmed. The additional work would verify that the assumptions made in the calculation of this generic background accidental aircraft crash rate were valid for that site.

15.8.5.3 Beyond Design Basis and Cliff-Edge Methodology for External Hazards [157]

ONR guidance in the SAPs [130] and TAG-13 [144] requires an assessment of the performance of the plant for more onerous considerations than those used for the design basis, i.e., for BDB conditions.

The BDB and Cliff-Edge methodology report describes the process to be followed when carrying out the BDB and Cliff- Edge external hazards assessment for the RR SMR. External hazards are defined in terms of their severity and frequency of occurrence.

The report explains the need for a BDB and Cliff-Edge assessment within national and international licensing context. It summarises relevant guidance and presents RGP on BDB and Cliff Edge assessments. Additionally, the report outlines the BDB and Cliff-Edge approach to be used for the RR SMR. In general, Cliff-Edges are addressed by investigating sensitivity around design basis using design margins. Significant BDB external hazards are addressed through design margins and the external hazards PSA. Discussion is provided on how non-discrete external hazards such as extreme temperature, wind and seismic events, and discrete external hazards such as accidental aircraft crash and industrial hazards should be considered.

The methodology will need to be applied by designers to demonstrate that BDB and Cliff-Edge margins are adequate and ensure robustness of hazards protections.

15.8.5.4 External Combined Hazards Methodology [151]

Refer to Section 15.8.2 for an overview of the external combined hazards methodology.

15.8.6 Protection Against External Hazards

15.8.6.1 Layout Optimisation to External Hazards

The Architectural and Layout Summary Report [114] states that SSCs that are required to deliver the FSF in RI following design basis or BDB external hazard events are protected by means of the Hazard Shield, the Seismic Isolation System (Aseismic Bearing) and redundancy & separation.

The Hazard Shield is a reinforced concrete structure which is designed to protect its contents from an aircraft impact event (see further discussion in the Aircraft Impact Design Philosophy and Methodology Statement [158]), as well as some of the other external hazards defined in the GB GSE [142] such as external explosions, wind loading, and wind-induced missiles.

The Seismic Isolation System is a series of reinforced concrete pedestals and aseismic bearings which support the reinforced concrete basemat, upon which the Hazard Shield and its contents sit. The Seismic Isolation System mitigates the effect of an earthquake to the Basemat by decoupling horizontal accelerations between the Basemat and the Raft Foundation [159].

The Hazard Shield is located on the Seismic Isolation System, meaning the contents (which will be seismically qualified as required) located within the Hazard Shield are subject to reduced horizontal accelerations due to seismic activity as well as the GSE external hazards. Further information on the design of the Hazard Shield and Seismic Isolation System is described in E3S Case Tier 1 Chapter 9B: Civil Engineering Works and Structures [120].

SSC tasked with delivering CoR functions such as Scram, Control Rods, Spent Fuel Storage Racks, and the ASF have been located within the Hazard Shield for external hazard protection. The exceptions to this statement are the ESWS trains and Back-up Generation System (BUGS), which are instead protected by separation, with their respective duplicate trains being situated North and South of the Hazard Shield structure.

It is claimed that following an aircraft impact, Safety Measures inside the Hazard Shield will remain functional to ensure the fulfilment of FSFs and at least one train of ESWS and BUGS will remain available to support associated Safety Measures through suitable separation. At RD7/DRP1, the individual trains of ESWS and BUGS are assumed to be located within a separate, seismically qualified structure which is still robust to site-wide external hazards such as external explosions, inclement weather and wind-driven missiles. The requirements and definitions of these structures will be matured in future design iterations.

The need for definition of mobile equipment and its role in long-term provision of safety functions such as top-up water supplies or mobile diesel generators will also be evaluated beyond RD7/DRP1. This equipment would similarly be anticipated to be stored in qualified structures.

SSC tasked with delivering CoFT functions such as PDHR, Low Temperature Decay Heat Removal, the SFP, SFP Cooling, SFP Boil Off are all located within the Hazard Shield for external hazard protection, except for ESWS and BUGS which support SFP Cooling and Low Temperature Decay Heat Removal (ESWS only).

SSC tasked with delivering CoRM functions such as the Containment Vessel, Containment Isolation Systems and Fuel Cladding are all located within the Hazard Shield for external hazard protection.

An Aircraft Impact Analysis and Design Report will be provided as the design matures (and a site is selected), which will underpin the design of the Hazard Shield for aircraft impact resistance, and contain an evaluation of plant performance due to the consequential hazards of impact-induced vibration and fire [158].

The Auxiliary Block at RD7/DRP1 is housed within a robust structure, which provides radiation protection to the external environment and protection of the Class 3 systems within from site-wide external hazards. Informed by the E3S requirements of the systems within, and following benchmarking against other plants and waste facilities, this structure is not expected to provide aircraft impact protection. Further work is identified to finalise the external hazard withstand requirements for the Auxiliary block, which may impact the level of protection required. For further details, see the Auxiliary and Waste Systems Layout Report [160].

As the RI layout and the hazard schedule is developed beyond RD7/DRP1, the layout design shall be optimised to ensure that the SMR is tolerant to all external hazards, including combined hazards. This will be achieved through verification of the Hazard Shield and Seismic Isolation functional requirements and assessment of the site and RI layout with regard to the hazard schedule and PSA.

15.8.6.2 Identification of External Hazard PIEs and FSFs

As discussed in Section 15.2.1, all credible external hazards PIEs for the RR SMR design are identified, fully defined and sentenced appropriately for analysis.

For all external hazard PIEs, the FSFs will be delivered across all levels of DiD by Safety Measures which deliver categorised High Level Safety Functions (HLSFs), through safety categorised functional requirements and non-functional requirements in the requirements management database [161].

External hazards requirements will be agreed and stored in the requirements management database where they will be allocated to the relevant teams to ensure that external hazard requirements are captured in the design process. The full process of identifying and integrating requirements will be finalised in a future iteration of the E3S Case.

15.9 Conclusions

15.9.1 Safety-Informed Design and ALARP

Safety assessments have been carried out with five 'lenses': design basis assessment, severe accident assessment, PSA, and internal and external hazards assessment. At RD7/DRP1, each of these five disciplines has fed safety insights into the ongoing design process, to provide confidence that risks can be reduced to ALARP.

Design basis provisions have been assessed by analysing several selected bounding faults that have informed safety categorisation of claimed safety measures, with consequent requirements for redundancy and diversity. The analyses have also informed trip settings and component sizing, so that the safety measures can meet the deterministic success criteria relevant to the plant state that needs to be achieved following a postulated fault. Analysis carried out so far provides high confidence that all credible design basis faults can be adequately protected with margin to the acceptance criteria.

The overall aims of the severe accident tasks are to demonstrate; that the Rolls-Royce SMR severe accident design provision reduces risks to ALARP, and the practical elimination of large or early releases. Where individual phenomena or event/ fault sequences are identified that challenge practical elimination targets, design enhancements will be evaluated to meet these targets where reasonably practicable. SAA demonstrates that, for the limited number of reasonably bounding event sequences assessed, the severe accident SSCs in place (as part of variant four of CSM [JM01]) are predicted to successfully prevent or mitigate severe accident phenomena associated with DEC-B for the analysis performed.

The PSA has been and is being used to risk-inform the design through optioneering and a RR SMR design decision process [162] is established to ensure that design optioneering takes account of quantitative techniques, including PSA, to gauge the impact of proposed decisions on nuclear safety risk. The PSA presented in Section 15.6 provides a prediction of the CDF from the Level 1 internal events at power PSA model, noting the sensitivities and conservatisms of the model at this stage. The use of PSA to inform the design from an early stage and the outputs of the PSA undertaken up to RD7/DRP1, provide confidence that risks are being iteratively assessed against numerical targets and can be reduced to ALARP.

The identification and analysis of internal hazards has iteratively informed the design of the RR SMR to provide (where reasonably practicable) inherent protection against internal hazards through optimisation of the layout. This includes segregation of the safety fluids trains by civil structures (as shown in the Safety Fluid Systems Layout Summary Report [163]) and segregation of EC&I trains by relocating into separate clusters (as shown in the Reactor Island EC&I Systems Layout Summary Report [164]). Safety measures are identified with safety categorised functional requirement assigned to SSCs through the fault schedule, providing confidence that the risk from internal hazards is tolerable and will be reduced to ALARP providing that the required hazard protection is in place.

External hazards and their combinations have been identified, and their magnitudes/loads have been quantified. The assessment has influenced the design, in particular, the civil structures. Generic methodologies have also been specified for several external hazard topics, which will be applied by designers during design development. This provides confidence that the RR SMR can demonstrate tolerance to external hazards and reduce risks to ALARP.

15.9.2 Assumptions and Commitments on Future Dutyholder / Licensee / Permit Holder

Table 15.9-1: Assumptions and Commitments on Future Dutyholder/Licensee/Permit Holder

Assumption/Commitment	ID	Description
Commitment	C15.1	The future dutyholder/licensee/permit holder shall identify all site specific external hazards and derive appropriate design basis values making allowances for climate change where applicable and provide a suitable safety justification once a site has been selected.
Commitment	C15.2	The future dutyholder/licensee/permit holder shall identify all site specific combined external hazards and provide a suitable safety justification.

15.9.3 Conclusions and Forward Look

The generic E3S Case objective at Version 2 is 'to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design' [3]. This confidence is built through development and underpinning of top-level claims across each chapter of the E3S Case, through supporting arguments and evidence. The top-level claim for chapter 15 is 'safety analysis informs the design and demonstrates there is suitable and sufficient defence in depth to deliver the fundamental safety functions, and that nuclear safety risks to workers and the public are reduced to ALARP'.

The arguments and evidence presented to meet the generic E3S Case objective at Version 2 are summarised in section 15.9.1 and cover design basis assessment, severe accident assessment, PSA, and internal and external hazards assessment.

Further arguments and evidence to underpin the claim will be developed in line with the E3S Case Route Map [4] and reported in future revisions of the generic E3S Case, which will further build confidence that the RR SMR can deliver its fundamental E3S objective. This will be done in the overall context of ALARP and is summarised below.

The design basis deterministic analysis will be widened out in scope to cover all fault scenarios and all modes of operation, and the performance models will continue to be updated based on the latest design information. Safety measures will be identified in a more detailed manner for faults in areas other than the reactor and at-power operation, including for shutdown modes, for the SFP, for fuel handling activities and for waste treatment and storage. Radiological consequence analysis for fault sequences will also be undertaken and evaluated against relevant acceptance criteria.

Further iterations of SAA will be undertaken for DEC-B, including assessment of a full suite of severe accident scenarios following RD8/DRP2. Validation activities will be undertaken using independent models to improve confidence in the SAA. Mechanical stress analysis will be undertaken to confirm that the RPV [JAA] has sufficient mechanical strength to maintain RPV [JAA] integrity during DEC-B. Uncertainty analysis will be undertaken based on RD8/DRP2, and radiological consequence assessments (Level 3 PSA and habitability studies) will be undertaken following RD9/DRP3 (using DRP1 and DRP2 design information). An update to the Practical Elimination arguments will be presented, considering any relevant updates to deterministic argument due to increased design maturity and probabilistic arguments.

The scope of the PSA will be significantly expanded so that the model continues to improve as a tool for a range of intended PSA applications, including risk-informed design and ALARP optioneering. The PSA model will include the following items:

- Operations with the reactor shutdown (Modes 3 -6b) (following RD7/DRP1).
- Sources of radiation other than the reactor core such as the fuel route, fuel storage, and SFP (following RD8/DRP2).
- Consideration of internal and external hazards (following RD8/DRP2).
- Level 2 PSA, meaning coverage of the severe accident phase and quantifying the frequency of radiological release (following RD8/DRP2).
- Level 3 PSA, meaning coverage of the radiological dispersal phase and quantifying the frequency of various health outcomes (following RD9/DRP3).
- Periodic update and validation against the latest reference designs (ongoing for RD8/DRP2 and RD9/DRP3).

Further work for internal hazard analysis on Reactor Island based on RD8/DRP2 will be undertaken and reflected in Version 3 of the E3S case. Additionally, analysis of internal/ external hazard combinations will be incorporated.

The external hazards analysis presented is applicable to the generic design of the RR SMR and a GSE for GB has been produced, along with analysis on combined external hazards, and methodologies on BDB, accidental aircraft crash, and space weather. Version 3 of the E3S case will incorporate further updates to the GSE and BDB methodology which will have inputs from other disciplines such as civils, and the combined external hazard reports which will consider the BDB methodology. Additionally, analysis of internal/external hazard combinations will be presented.

15.10 References

[1] Rolls-Royce SMR Limited, SMR0004247 Issue 3, "E3S Case Tier 1 Chapter 13: Conduct of Operations," May 2024.

[2] Rolls-Royce SMR Limited, SMR0004555 Issue 3, "E3S Case Tier 1 Chapter 16: Operational Limits and Conditions," May 2024.

[3] Rolls-Royce SMR Limited, SMR0004294 Issue 3, E3S Case Tier 1 Chapter 1: Introduction, May 2024.

[4] Rolls-Royce SMR Limited, SMR0002155/003, E3S Case Route Map, November 2023.

[5] Rolls-Royce SMR Limited, SMR0001603/001, "Environmental, Safety, Security and Safeguarding Design Principles," August 2022.

[6] IAEA, "SSG2 Deterministic Safety Analysis for Nuclear Power Plants," 2019.

[7] W. RHWG, "Practical Elimination Applied to New NPP Designs - Key Elements and Expectations," September 2019.

[8] IAEA, "SSG-68 IAEA Safety Standards, Design of Nuclear Installations Against External Events Excluding Earthquakes," 2021.

[9] IAEA, NS-G-1.5, "External Events Excluding Earthquakes in the Design of Nuclear Power Plants," November 2003.

[10] "IAEA-TECDOC-1944, Fire Protection in Nuclear Power Plants".

[11] Rolls-Royce SMR Limited, SMR0004589 Issue 3, "E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs," May 2024.

[12] Rolls-Royce SMR Limited, "E3S Case Chapter 6: Engineered Safety Systems, SMR0003771/002," RR SMR, Warrington, 2024.

[13] Rolls-Royce SMR Limited, "Rolls-Royce SMR Hazard Identification Strategy, SMR0001228/002," Rolls-Royce SMR Limited, Derby, United Kingdom, July 2023.

[14] Rolls-Royce SMR Limited, SMR0009098 Issue 1, "External Hazard Identification and Analysis Standard," April 2024.

[15] Rolls-Royce SMR Limited, SMR0009097 Issue 1, "Internal Hazard Identification and Analysis Standard," April 2024.

[16] Rolls-Royce SMR Limited, "Rolls-Royce SMR Hazard Log Report - Version 7, SMR0001317/004," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[17] Rolls-Royce SMR Limited, "Rolls-Royce SMR Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies, SMR0001389/004," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[18] Rolls-Royce SMR Limited, SMR0006219/001, "Severe Accident Analysis Summary Report," 2023.

[19] Rolls-Royce SMR Limited, "Rolls-Royce SMR Fault Schedule (Version 7), SMR0004444/003," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[20] Rolls-Royce SMR Limited, "Rolls-Royce SMR Deterministic Safety Case - Methodologies, SMR0000531/002," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[21] Rolls-Royce SMR Limited, "Safety Measures Module, SMR0004917/002," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[22] Rolls-Royce SMR Limited, "RR SMR E3S Design Basis Deterministic Safety Assessment Summary, SMR0009855/001," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[23] Rolls-Royce SMR Limited, "Reactor Plant Performance Fault Study Analysis Summary, SMR0007538/001," Rolls-Royce SMR Limited, Derby, United Kingdom, November 2023.

[24] Rolls-Royce SMR Limited, "ALARP Summary Report, SMR0009086/001," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[25] Rolls-Royce SMR Limited, "UK SMR Alarp and BAT Position Paper, Reactor Heatsinks, EDNS01000953979/001," Rolls-Royce SMR Limited, Derby, United Kingdom, March 2021.

[26] Rolls-Royce SMR Limited, "System Design Description for the Reactor Coolant System, SMR0000402/003," Rolls-Royce SMR Limited, Derby, United Kingdom, October 2023.

[27] Rolls-Royce SMR Limited, "Justification of Design Limits - Fuel and Core, SMR0005456/002," Rolls-Royce SMR Limited, Derby, United Kingdom, January 2024.

[28] Rolls-Royce SMR Limited, "Safety Measure Design Description for the Containment [JM01] Safety Measure, SMR0008536/001," Rolls-Royce SMR Limited, Derby, United Kingdom, November 2023.

[29] ONR, "Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1," January 2020.

[30] EUR, "Generic Nuclear Island Requirement: Chapter 1 Safety Requirements (Volume 2), Rev. E," 2016.

[31] IAEA, INSAG-12, "Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3, Rev. 1," 1999.

[32] US NRC, "New Light-Water Reactors," 11 October 2022. [Online]. Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp/reactor-safety-new.html. [Accessed 3 March 2023].

[33] Rolls-Royce SMR Limited, "Environment, Safety, Security & Safeguards Case Chapter 18: Human Factors Engineering, SMR0004520/002," Rolls-Royce SMR Limited, Derby, United Kingdom, February 2024.

[34] Rolls-Royce SMR Limited, SMR0004734 Issue 2, "PSA Technical Requirements," January 2024.

[35] Rolls-Royce SMR Limited, "Reactor Plant Performance Design Basis Analysis Methodology, SMR0006250/002," Rolls-Royce SMR Limited, Derby, United Kingdom, November 2023.

[36] IAEA, "IAEA SSG-2 Deterministic Safety Analysis for Nuclear Power Plants," IAEA, Vienna, 2019.

[37] EUR, "European Utility Requirements LWR Nuclear Power Plants Volume 2 Generic Nuclear Island Requirements, Chapter 4: Design Basis, Revision E," October 2016.

[38] European Utility Requirements (EUR) for LWR NNP, "Generic and Nuclear Island Requirements," Revision E 2016.

[39] United States Nuclear Regulatory Commission, "10 CFR Parts 50 and 52 Performance based emergency core cooling systems cladding acceptance criteria - Federal Register, vol.79, no. 56," 2014.

[40] United States Nuclear Regulatory Comission, "10 CFR § 50.46 Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors," 2021.

[41] Westinghouse Electric Company LLC, "AP1000® pre-construction safety report - UKP-GW-GL-793NP, Revision 1," 2017.

[42] Office for Nuclear Regulation, "Generic Design Assessment - new civil reactor build: Step 4 fault studies - design basis faults assessment of the Westinghouse AP1000® reactor - ONR-GDA-AR-11-004a," 2011.

[43] AREVA NP and EDF SA, "UK EPR PCSR - Sub-chapter 14.0 - assumptions and requirements for the PCC accident analyses - UKEPR-0002-140 Issue 05," 2012.

[44] AREVA NP and EDF SA, "UK EPR PCSR - Sub-chapter 16.1 - risk reduction analysis (RRC-A) - UKEPR-0002-161 Issue 07," 2012.

[45] Office for Nuclear Regulation, "Generic Design Assessment - new civil reactor build: Step 4 fault studies - design basis faults assessment of the EDF and AREVA UK EPR™ reactor," ONR-GDA-AR-11-020a," 2011.

[46] Rolls-Royce SMR Limited, "Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Summary, SMR0007874/001," Rolls-Royce SMR Limited, Derby, United Kingdom, October 2023.

[47] Rolls-Royce SMR Limited, SMR0005193 Issue 1, " Reactor Physics Validation," June 2023.

[48] Rolls-Royce SMR Limited, "Design Basis Radiological Consequences Assessment Methodology, SMR0010027," Rolls-Royce SMR Limited, Derby, United Kingdom, February 2024.

[49] Rolls-Royce SMR Limited, "Environment, Safety, Security and Safeguards Case Chapter 12: Radiation Protection, SMR0004139/002," Rolls-Royce SMR Limited, Derby, United Kingdom, February 2024.

[50] Rolls-Royce SMR Limited, SMR0006141_002, "Severe Accident MAAP Methodology Report," 2023.

[51] Rolls-Royce SMR Limited, SMR0007874_001, "Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Summary," 2023.

[52] Rolls-Royce SMR Limited, SMR0005258, Issue 1, "SA Management Strategy," May 2023.

[53] IAEA, "IAEA Safety Reports Series No. 56 - Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants," IAEA, Vienna, 2008.

[54] SARNET, "Nuclear Safety in Light Water Reactors - Severe Accident Phenomenology," Elsevier, Amsterdam, 2012.

[55] NEA, "High Pressure Melt Ejection (HPME) and Direct Containment Heating (DCH) State of the Art Report," NEA, Issy-les-Moulineaux, 1996.

[56] NUREG, "NUREG/CR-5373: A Demonstration Experimemt of Steam-Driven, High-Pressure Melt Ejection," US NRC, Albuquerque, 1999.

[57] Rolls-Royce SMR Limited, SMR0008536_001, "Safety Measure Design Description for the Containment Safety Measure [JM01]," November 2023.

[58] NEA, "In-Vessel and Ex-Vessel Hydrogen Sources," NEA, 2001.

[59] IAEA, "TECDOC-1661: Mitigation of Hydrogen Hazards in Severe Accidents in Nuclear Power Plants," IAEA, Vienna, 2011.

[60] e. a. D. Magallon, "Results of Phase 1 of OECD Programme SERENA on Fuel Coolant Interaction," ERMSAR, Aix-en-Provence, 2005.

[61] ASAMPSA2, "Best Practices Guidelines for PSA Development & Applications, Vol 2 - Best practices for the GENII PWR, GEN II BWR L2 PSAs. Technical Report ASAMPSA2/WP2-3/D3.3/2013-35," ASAMPSA2, 2013.

[62] Nuclear Energy for New Europe, "Simulation of Ex-Vessel Steam Explosion in PWR Reactor Cavity," IAEA, Ljubljana, 2005.

[63] NEA, "State-of-the-art Report on Molten Corium Concrete Interaction and Ex-Vessel Molten Core Coolability," OECD, 2017.

[64] IAEA, "Safety Report Series No 56, Approaches and tools for SAA for NPPs," 2008.

[65] Rolls-Royce SMR Limited, "Accident Chemistry Strategy Report, SMR0008800/001," RR SMR, Derby, 2023.

[66] Rolls-Royce SMR Limited, SMR0006215/001, "MAAP Model Parameter Settings v1.0.2," 2023.

[67] Rolls-Royce SMR Limited, SMR0004993/002, "JM01-R Requirements Specification for the Containment Safety Measure," 2023.

[68] Rolls-Royce SMR Limited, "E3S Case Chapter 20: Chemistry, SMR0004982/002," RR SMR, Derby, 2024.

[69] Rolls-Royce SMR Limited, SMR0005922_2, "System Description for In-Vessel Retention Function and Reactor Cavity Injection [JNM]," 2023.

[70] Rolls-Royce SMR Limited, "E3S Case Chapter 8: Electrical Power, SMR0004010/002," RR SMR, Warrington, 2023.

[71] "JM01-R Requirements Specification for the Containment Safety Measure [JM01], SMR0004993 Issue 2," Nov 2023.

[72] Rolls-Royce SMR Limited SMR0006184_002, "System Design Description for the Hydrogen Reduction System (HRS) [JMT]," 2023.

[73] Rolls-Royce SMR Limited, "JMT-R: Requirements Specification for the Hydrogen Reduction System [JMT], SMR0006283/002," RR SMR, Warrington, 2023.

[74] Rolls-Royce SMR Limited, SMR0000601_002, "Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Strategy," 2023.

[75] Rolls-Royce SMR Limited, EDNS01000470763/005, "Fault Schedule Report," 2021.

[76] Rolls-Royce SMR Limited, SMR0006357_001, "Phenomena Identification and Ranking Tables (PIRT) for Severe Accident Analysis," 2023.

[77] Rolls-Royce SMR Limited, SMR0006213_001, "Test and Assessment Matrix (TAM) for Severe Accident Analysis Using the MAAP5 code," 2023.

[78] Rolls-Royce SMR Limited, SMR0005197, "MAAP Model Development Report," 2023.

[79] Rolls-Royce SMR Limited, "Severe Accident Assessments for Containment Cooling and Spray Function for RD7, SMR0008874/001," RR SMR, Warrington, 2023.

[80] Office for Nuclear Regulation, “Nuclear Safety Technical Assessment Guide - Chemistry Assessment, NS-TAST-GD-089/1.1,” ONR, Bootle, 2022.
[81] Rolls-Royce SMR Limited, SMR0007629 Issue 1, “Severe Accident Off-site Consequence Methodology,” September 2023.
[82] “International Atomic Energy Agency, Assessment of the Safety Approach for Design Extension Conditions and Application of the Concept of Practical Elimination in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-88 [IAEA Preprint]”.
[83] Rolls-Royce SMR Limited, “RR SMR Practical Elimination report,” expected in Feb 2025.
[84] Rolls-Royce SMR Limited, SMR0004444 Issue 3, “RR SMR Fault Schedule (version 7),” January 2024.
[85] International Atomic Energy Agency, “Assessment of the Safety Approach for Design Extension Conditions and Application of the Concept of Practical Elimination in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-88 [IAEA Preprint],” 2023.
[86] Rolls-Royce SMR Limited, SMR0006518_001, “RR SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method,” 2023.
[87] Rolls-Royce SMR Limited, SMR0004363 Issue 3, “E3S Case Tier 1 Chapter 23: Structural Integrity,” May 2024.
[88] Rolls-Royce SMR Limited, IMS Process C3.2.2-9, “Refinement of Safety Classification of Structures and Mechanical Components”.
[89] Rolls-Royce SMR Limited, SMR0005677 Issue 1, “System Design Description for the Fuel Pool Fluid Systems,” July 2023.
[90] Rolls-Royce SMR Limited, SMR0004735 Issue 2, “PSA Development Strategy,” January 2024.
[91] Rolls-Royce SMR Limited, SMR0001204 Issue 1, “Rolls-Royce Small Modular Reactor Master Records Index - Reference Design 5 - In Support of Preliminary Concept Definition,” June 2022.
[92] Rolls-Royce SMR Limited, SMR0004916 Issue 1, “Rolls-Royce SMR Fault Schedule Module Version 6,” March 2023.
[93] Rolls-Royce SMR Limited, SMR0001389 Issue 3, “Rolls-Royce SMR Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies,” April 2023.
[94] Rolls-Royce SMR Limited, SMR0007297 Issue 1, “Rolls-Royce Small Modular Reactor - Master Records Index - Reference Design 6 - In Support of the Final Concept Definition,” July 2023.
[95] Rolls-Royce SMR Limited, SMR0005020 Issue 2, “Rolls-Royce SMR Control and Instrumentation Engineering Schedule,” June 2023.
[96] Rolls-Royce SMR Limited, SMR0008732 Issue 1, “PSA Assessment of Limitations,” January 2024.
[97] Rolls-Royce SMR Limited, SMR0008850 Issue 1, “Probabilistic Safety Assessment Main Report,” January 2024.
[98] Rolls-Royce SMR Limited, SMR0005508 Issue 1, “Probabilistic Safety Assessment (PSA) Event Sequence Modelling Methodology,” April 2023.
[99] Rolls-Royce SMR Limited, SMR0008247 Issue 1, “Probabilistic Safety Assessment (PSA) Event Sequence Modelling Report,” October 2023.
[100] Rolls-Royce SMR Limited, SMR0006322 Issue 1, “Probabilistic Safety Assessment (PSA) Human Based Safety Claims (HBSC) Modelling Methodology,” June 2023.
[101] Rolls-Royce SMR Limited, SMR0008148 Issue 1, “PSA Operator Actions Modelling Report,” October 2023.
[102] Rolls-Royce SMR Limited, SMR0006323 Issue 1, “Probabilistic Safety Assessment (PSA) Structures, Systems and Components (SSC) Modelling Methodology,” April 2023.
[103] Rolls-Royce SMR Limited, SMR0008526 Issue 1, “Probabilistic Safety Assessment (PSA) Structures, Systems and Components (SSC) Modelling Report,” October 2023.
[104] Rolls-Royce SMR Limited, SMR0006379 Issue 1, “PSA Data Methodology,” June 2023.
[105] Rolls-Royce SMR Limited, SMR0007938 Issue 1, “PSA Data Notebook,” October 2023.
[106] Rolls-Royce SMR Limited, SMR0008733 Issue 1, “PSA Hazard Event Modelling Methodology,” December 2023.

[107] Rolls-Royce SMR Limited, SMR0006900 Issue 1, “UK SMR Reactor Island Operating Philosophy,” August 2023.

[108] Idaho National Laboratory, INL/EXT-21-65055, “Industry-Average Performance for Components and Initiating Events at U.S Commercial Nuclear Power Plants: 2020 Update,” November 2021.

[109] Idaho National Laboratory, INL/EXT-21-62940, Revision 1, "CCF Parameter Estimations, 2020 Update", August 2022.

[110] Idaho National Laboratory, INL/RPT-23-72818, "Initiating Event Rates at U.S. Nuclear Power Plants: 2022 Update", June 2023.

[111] Rolls-Royce SMR Limited, SMR0008861 Issue 1, “PSA Issues Log,” October 2023.

[112] Rolls-Royce SMR Limited, EDNS01000966510/001, “PSA Risk Spectrum model V1.0 reflecting the design as baselined at Decision 21 and Decision 22,”, May 2021.

[113] Rolls-Royce SMR Limited, SMR0005529 Issue 1, “Internal Hazards Strategy,” 2023.

[114] Rolls-Royce SMR Limited, SMR0007298/005, “Reactor Island Architectural and Layout Summary Report,” January 2024.

[115] Rolls-Royce SMR Limited, SMR0006411 Issue 1, “Internal Hazards Methodology,” 2023.

[116] Rolls-Royce SMR Limited, SMR0007172 Issue 1, “Internal Hazards Summary Report - Reactor Island within Hazard Shield,” 2024.

[117] Rolls-Royce SMR Limited, SMR0008560 Issue 1, “Internal Hazards Summary Report - Outside Hazards Shield,” 2024.

[118] Rolls-Royce SMR Limited, SMR0007173 Issue 1, “Internal Combined Hazards Methodology and Identification Report,” 2023.

[119] Rolls-Royce SMR Limited, SMR0008225 Issue 1, “Area Datasheets,” 2024.

[120] Rolls-Royce SMR Limited, SMR0003778 Issue 3, “E3S Case Tier 1 Chapter 9B: Civil Engineering Works and Structures,” May 2024.

[121] Rolls-Royce SMR Limited, SMR0008525 Issue 1, “Approach to Design Verification for Internal Hazards,” 2024.

[122] IAEA, “Protection against Internal Hazards in the Design of Nuclear Power Plants SSG-64,” 2021.

[123] Rolls-Royce SMR Limited, SMR0010037 Issue 1, “Internal Hazards Transverse Requirements and Design Considerations,” 2024.

[124] Rolls-Royce SMR Limited, SMR0009446 Issue 1, “Internal Hazards Analysis - Reactor Island within Hazard Shield,” 2024.

[125] Rolls-Royce SMR Limited, SMR0006803 Issue 1, “Internal Hazards Fire Analysis Report,” 2023.

[126] Rolls-Royce SMR Limited, SMR0009983 Issue 1, “Internal Hazards Analysis - Outside Hazard Shield,” 2024.

[127] S. G. a. P. J. Dolan, The Effects of Nuclear Weapons (Online Edition), Chris Griffith and Eric A. Meyer, 2022.

[128] Rolls-Royce SMR Limited, SMR0008277 Issue 2, “MKoP Primary Structure Standard Frame Design Definition,” 2024.

[129] Rolls-Royce SMR Limited, SMR0008827 Issue 1, “Modularisation Kit of Parts Barriers Design Definition,” 2024.

[130] ONR, “Safety Assessment Principles for Nuclear Facilities, Revision 1,” 2020.

[131] Rolls-Royce SMR Limited, SMR0004542 Issue 3, “E3S Case Tier 1 Chapter 2: Generic Site Characteristics,” May 2024.

[132] Rolls-Royce SMR Limited, EDNS01000475199/002, “Definition of Design Basis for Internal/External Hazards,” 2017.

[133] Rolls-Royce SMR Limited, SMR0001317/004, “Hazard Log Report,” October 2022.

[134] ONR, “NS-TAST-GD-013, Nuclear Safety Technical Assessment Guide 13: External Hazards, Revision 8.1,” December 2022.

[135] WANO, “Safety of New NPP designs. Study by Reactor Harmonization Working Group RHWG,” March 2013.

[136] US NRC, NUREG-1407, “Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities,” June 1991.
[137] US NRC, “NUREG/CR-2300 A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,” 1983.
[138] Rolls-Royce SMR Limited, EDNS01000965477/001, “External Hazards Review,” May 2021.
[139] SKI, “ISSN 1104–1374, ISRN SKI-R-02/27-SE Guidance for External Events Analysis, 02:27,” February 2003.
[140] European Commission Seventh Framework, Advanced Safety Assessment Methodologies: Extended PSA (ASAMPSA_E), “Technical report ASAMPSA_E /WP21/D21.2/2017-41 List of External Hazards to be Considered in ASAMPSA_E,” 2017.
[141] OECD-NEA, “Probabilistic Safety Analysis (PSA) of Other External Events than Earthquake, NEA/CSNI/R(2009),” March 2009.
[142] Rolls-Royce SMR Limited, SMR0001535/002, “RR SMR GB Generic Site Envelope,” 2023.
[143] ONR, “ONR-GDA-GD-007 New Nuclear Power Plants: Generic Design Assessment, Technical Guidance, Revision 0,” May 2019.
[144] ONR, “NS-TAST-GD-013, Nuclear Safety Technical Assessment Guide 13: External Hazards, Revision 9,” October 2023.
[145] ONR, “NS-TAST-GD-013 Annex 2 - Meteorological Hazards,” October 2023.
[146] ONR, “NS-TAST-GD-013 Annex 1 - Seismic Hazards,” November 2021.
[147] ONR, “NS-TAST-GD-013 Annex 4 - Accidental Aircraft Crash Hazard,” November 2021.
[148] ONR, “NS-TAST-GD-013 Annex 5 - Other External Hazards,” November 2023.
[149] ONR , “NS-TAST-GD-013 Annex 3 - Coastal Flood Hazards,” October 2023.
[150] “UK Climate Projections (UKCP),” Met Office, [Online]. Available: https://www.metoffice.gov.uk/research/approach/collaboration/ukcp/index. [Accessed July 2022].
[151] Rolls-Royce SMR Limited, SMR0009084/001, “External Combined Hazards,” December 2023.
[152] Rolls-Royce SMR Limited, SMR0008879/001, “Space Weather Hazard Methodology,” December 2023.
[153] Rolls-Royce SMR Limited, SMR0007038/002, “Analysis of Background Accidental Aircraft Crash Frequency,” November 2023.
[154] J. Byrne, The calculation of aircraft crash risk in the UK, Health and Safety Executive, 1997.
[155] Z. Chaplin, “Update of aircraft crash rates used by HSE in assessing hazards from chemical, process and other major hazard installations. Research Report RR1140,” Health and Safety Executive, December 2019. [Online]. Available: https://www.hse.gov.uk/research/rrpdf/rr1140.pdf.
[156] Air Accidents Investigation Branch, “Air Accidents Investigation Branch reports,” [Online]. Available: https://www.gov.uk/aaib-reports.
[157] Rolls-Royce SMR Limited, SMR0009352/001, “Beyond Design Basis and Cliff-Edge Methodology for External Hazards,” January 2024.
[158] Rolls-Royce SMR Limited, SMR0005709/001, “Aircraft Impact Design Philosophy and Methodology Statement,” 2023.
[159] Rolls-Royce SMR Limited, SMR0005690/002, “Design Basis for Reactor Island Structures,” 2023.
[160] Rolls-Royce SMR Limited, SMR0008314/001, “Auxiliary and Waste Systems Layout Summary Report,” January 2024.
[161] Rolls-Royce SMR Limited, SMR0000627/002, “E3S Case Development and Management Arrangements,” November 2023.
[162] Rolls-Royce SMR Limited, TS-DD-02/006, SMR Decision Record, 2023.
[163] Rolls-Royce SMR Limited, SMR0008120 Issue 1, “Safety Fluid Systems Layout Summary Report,” 2024.
[164] Rolls-Royce SMR Limited, SMR0008140 Issue 1, “Reactor Island EC&I Systems Layout Summary Report,” 2024.
[165] Rolls-Royce SMR Limited, “System Design Description - Automatic Depressurisation System [JNF], SMR0005186/002,” RR SMR, Warrington, 2023.

[166] Rolls-Royce SMR Limited, “System Design Description - Reactor Coolant Pressure Relief System [JEG], SMR0005891/002,” RR SMR , Warrington, 2023.

[167] Rolls-Royce SMR Limited, “E3S Case Chapter 7: Instrumentation & Control, SMR0003929/002,” RR SMR , Warrington, 2023.

[168] Rolls-Royce SMR Limited, EDNS01000887611/001, “UK SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method,” August 2021.

[169] Rolls-Royce SMR Limited, SMR0007538 Issue 1, “Reactor Plant Performance Fault Study Analysis Summary,” October 2023.

[170] Rolls-Royce SMR Limited, SMR0006219 Issue 1, “Severe Accident Summary Report,” October 2023.

15.11 Appendix A: Claims, Arguments, Evidence

Table 15.11-1: Mapping of Claims to Chapter Sections provides a mapping of the claims to the corresponding sections of the chapter that summarise the arguments and/or evidence. The full decomposition of claims and link to underpinning Tier 2 and Tier 3 information containing the detailed arguments and evidence is presented in the E3S Case Route Map [4].

Table 15.11-1: Mapping of Claims to Chapter Sections

Claim	Section of Chapter 15 containing Arguments / Evidence summary
Design Basis Fault Studies	
Systematic hazard identification exercises are employed to identify hazards	15.2.1
Hazards are sentenced appropriately for analysis	15.2.1
Identification of PIEs is supplemented by reviews of RGP and industry guidance	15.2.1
Hazards are grouped according to plant response and fault progression/consequences	15.2.1, 15.2.3
PIE definition covers all modes of operation and all types of fault on all areas of the plant, covering all sources of radioactivity	15.2.3
Initiating event frequencies have been identified using a consistent and systematic means, and are best estimate values	15.2.1, 15.2.4
HLSFs are identified for each PIE at each level of defence in depth, aligned to each Fundamental Safety Function	15.2.6
At least one Safety Measure is assigned to deliver HLSFs for infrequent faults	15.2.6
At least two Diverse Safety Measures are assigned to deliver HLSFs for high consequence frequent faults	15.2.6
Safety Measure design principles and deterministic safety rules are adhered to in the design of safety measures which fulfil the HLSFs	See E3S Case Tier 1 Chapter 3 [11]
SSCs that comprise Safety Measures delivering HLSFs are assigned Safety Categorised Functional Requirements and classified accordingly	15.2.7
Human actions that the operator needs to take to monitor the initiation and operation of SSCs are defined and classified according to the safety category of the HLSF being delivered	15.2.6
Computer codes and models used for deterministic analysis are validated	15.5.1.2

Claim	Section of Chapter 15 containing Arguments / Evidence summary
Acceptance Criteria for Design Basis Performance Analysis Design Basis (DBC 1, 2i, 2ii, 3i and 3ii) are defined and justified with suitable margin	15.3.2
The scope of the DBC-1 and DBC-2 analysis is informed by the Fault Schedule, with bounding PIEs justified and modelled	15.5.2
The scope of the DBC-2ii/3i/3ii/4 analysis is informed by the Fault Schedule, with bounding PIEs justified and modelled	15.5.3
The scope of the DEC-A analysis is informed by the Fault Schedule, with bounding PIEs justified and modelled	15.5.4
Deterministic analysis of spent fuel pool faults (plant state DBC-1 to DEC-A) demonstrates that all relevant acceptance criteria are met and risks are ALARP	15.5.6
Deterministic analysis of Fuel Handling faults (plant state DBC-1 to DEC-A) identified in the Fault Schedule demonstrates that all relevant acceptance criteria are met and risks are ALARP	15.5.7
Fault analysis is used, where appropriate, to inform the design	15.5.1.5
Fault analysis is used, where appropriate, to inform operating procedures	15.2.6.1
DECs with core melt (plant state DEC-B)	
Acceptance Criteria for Performance Analysis are defined and justified with suitable margin such that a safe and stable state is delivered	15.3.1
A comprehensive fault and hazard analysis has been used to identify the CSM and its subfunctions associated with severe accident mitigative.	0
CSM subfunction (DEC-B severe accident mitigative measures) have been identified holistically based on an understanding of severe accident phenomena and progression related to the RR SMR.	15.5.5.4 and 15.5.5.5
The CSM variant 4 subfunctions are designed to survive conditions expected within DEC B.	Analysis to be provided following DRP2
Safety analysis informs the design of the CSM variant 4 subfunctions (severe accident mitigative systems)	0
The IVR (In Vessel Retention) function will retain core melt in the event of DEC-B.	15.5.5.6.2
The SAD (Severe Accident Depressurisation) function will avoid a HPME and DCH in the event of a severe accident.	15.5.5.6.3

Claim	Section of Chapter 15 containing Arguments / Evidence summary
The hydrogen reduction system will reduce the hydrogen risks associated with in-vessel phenomena to a safe level that will not challenge the integrity of containment in the event of DEC-B	15.5.5.6.4
The Containment Heat Removal subfunction will provide sufficient cooling/pressure reduction of the containment atmosphere in the event of DEC-B	15.5.5.6.1
Deterministic analysis of design extension conditions with core melt (plant state DEC-B) has been carried out to identify further risk reduction measures	To be considered following DRP2
Radionuclide retention and transportation within the RR SMR (taking into account safety features and design) are analysed to support source term development	To be considered following DRP2
The chemical form of Iodine and other volatiles during a severe accident are identified to support level 3 PSA	To be considered following DRP2
Energetic severe accident phenomena which can directly result in containment failure are practically eliminated.	15.5.5.9
Expected DEC B severe accident phenomena are unlikely to challenge containment integrity with a high degree of confidence.	15.5.5.9
Severe Accident phenomena resulting from the SFP are demonstrated as extremely unlikely to occur with a high degree of confidence.	15.5.5.9
All radiological acceptance criteria relevant to Severe Accidents are met.	15.5.5.8
Radiological Consequences	
Design basis radiological consequences carried out on a representative set of bounding faults	15.5.8.1
Radcons codes are validated	15.5.1.2
Dispersion and foodchain modelling, exposure pathways are appropriate for the range of sites under consideration	15.5.8.1
Target 4 (project equivalent) is met	15.5.8.1
DB Radcons influences the design	15.5.8.1
Probabilistic Safety Assessment	
The probabilistic safety assessment considers all initiating events with potential to cause radiological exposure to people on-site or off-site.	15.6.1.3
The probabilistic safety assessment considers all significant sources of radiation on the site.	15.6.1.2

Claim	Section of Chapter 15 containing Arguments / Evidence summary
The probabilistic safety assessment considers all permitted operating states of the site.	15.6.1.3
The probabilistic safety assessment is based on best estimate approaches wherever practicable.	15.6.1.3
The probabilistic safety assessment provides an adequate representation of the design, its behaviour, and its operation.	15.6.1.2 and 15.6.1.3
The probabilistic safety assessment is used, where appropriate, to inform the design of the site and its facilities.	15.6.5
The probabilistic safety assessment is used, where appropriate, to inform the operation of the site and its facilities.	15.6.5
The probabilistic safety assessment is used, where appropriate, to inform emergency planning.	15.6.5
The probabilistic safety assessment is used, where appropriate, to inform the provision of measures to mitigate the potential for significant radiological consequences.	15.6.3
The probabilistic safety assessment is used, where appropriate, to inform qualification requirements.	15.6.5
The probabilistic safety assessment quantifies the frequency of significant fuel damage, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	15.6.2
The probabilistic safety assessment quantifies the frequency of large or early release, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	15.6.3
The probabilistic safety assessment quantifies the frequency of death of a person on the site from accidents at the site resulting in exposure to ionising radiation, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	15.6.4
The probabilistic safety assessment quantifies the frequency of any single accident giving an effective dose to any person on-site, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	15.6.4
The probabilistic safety assessment quantifies the frequency of death of a person off the site from accidents at the site resulting in exposure to ionising	15.6.4

Claim	Section of Chapter 15 containing Arguments / Evidence summary
radiation, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	
The probabilistic safety assessment quantifies the frequency of accidents giving an effective dose to any person off-site, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	15.6.4
The probabilistic safety assessment quantifies the frequency of 100 or more fatalities from accidents at the site resulting in exposure to ionising radiation, assesses it against project risk targets, and demonstrates that it has been reduced to ALARP.	15.6.4
Internal Hazards	
The approach to ensure tolerance to internal hazards is based on RGP and OPEX.	15.7.3.6
The individual internal hazards and hazard combinations that can potentially cause initiating faults and thus affect nuclear safety are sufficiently identified.	Table 15.7-2: Internal Hazards Outputs from Fault Schedule
The safety measures to mitigate the consequences of internal hazards are sufficiently identified and classified accordingly	15.2.6
The layout is optimised to eliminate or minimise the risks of internal hazards (including combined hazards)	15.7.5.1
The modularisation approach is optimised to eliminate or minimise the risks of internal hazards (including combined hazards)	15.7.5.2
Analysis demonstrates that Reactor Island Within Hazard Shield is tolerant to Internal Hazards (including Combined Hazards)	15.7.4
Analysis demonstrates that Reactor Island outside Hazard Shield is tolerant to Internal Hazards (including Combined Hazards)	15.7.4
Internal Hazards Safety Measures are substantiated to achieve their Safety Categorised Functional Requirements	15.7.5.3
External Hazards	
All appropriate external hazards for a Great Britain site have been identified and screened.	15.8.2
All credible external hazards PIEs for the RR SMR design are identified, fully defined and sentenced appropriately for analysis.	15.2.3

Claim	Section of Chapter 15 containing Arguments / Evidence summary
For all external hazards Postulated Initiating Events (PIEs), the Fundamental Safety Functions are delivered across all levels of defence in depth by Safey Measures which deliver categorised High Level Safety Functions (HLSFs).	TBC – discussion provided in Section 15.8.4
Methodologies for SSC design and analysis, including civil structures are developed.	15.8.4 See also Chapter 9B of the E3S Case
The layout is optimised to eliminate or minimise the risks of external hazards (including combined hazards).	15.8.4
Beyond Design Basis and Cliff-Edge margins are adequate and ensure robustness of hazards protection.	TBC – discussion provided in Section 15.8.4
External Hazards Safety Measures are substantiated to achieve their Safety Categorised Functional Requirements.	TBC – discussion provided in Section 15.8.4. See also Chapter 3 of the E3S Case
Internal and external hazard combinations and consideration of external combined hazards beyond the design basis are currently excluded but will be considered in Step 3 of GDA.	15.8.3

15.12 Appendix B: RR SMR PIE List

This appendix lists all the PIEs that have been identified as applicable to the RR SMR design.

RR SMR PIE
ICF.1.1.01: Complete Loss of Pumped Primary Flow
ICF.1.1.02: Partial or Recoverable Loss of Pumped Primary Flow
ICF.1.1.03: Reactor Coolant Pump Shaft Seizure (Locked Rotor)
ICF.1.2.01: Excessive Primary Pressure due to Spurious Initiation of Reactor Coolant Pump(s)
ICF.2.1.01: Primary Pressure Decrease due to Pressuriser Heaters Failing Off
ICF.2.1.02: Primary Pressure Decrease due to Spurious Initiation of Pressuriser Spray
ICF.2.2.01: Primary Pressure Increase due to Heaters Fail On
ICF.2.2.02: Primary Pressure Increase due to Excessive Operation of Chemical Volume Control System
ICF.2.2.03: Primary Pressure Increase due to Failure to Letdown
ICF.2.2.04: Excessive Primary Pressure due to Spurious Initiation of High Pressure Injection System
ICF.3.1.01: Spurious Scram
ICF.3.1.02: Reactivity Control Imbalance
ICF.3.1.03: Spurious Initiation of Alternative Shutdown Function
ICF.3.2.01: Excessive Control Rod Bank Withdrawal
ICF.3.2.02: Excessive Steam Demand due to Large Isolable Steam Leak
ICF.3.2.03: Excessive Steam Demand due to Large Un-Isolable Steam Leak
ICF.3.2.04: Excessive Steam Demand due to Steam Generator Rupture
ICF.3.2.05: Temperature Reduction of Feedwater Supply
ICF.3.2.06: Excessive Steam Demand due to Spurious Steam Generator Relief Valve Lift
ICF.3.2.07: Excessive Steam Demand due to Spurious Atmospheric Steam Dump Activation
ICF.4.1.01: Complete Loss of Steam Generator Feed
ICF.4.1.02: Partial Loss of Steam Generator Feed
ICF.4.1.03: Loss of Duty Steam Generator Feed
ICF.4.1.04: Un-isolable Feedwater Line Break
ICF.4.2.01: Excessive Feedwater Supply
ICF.5.1.01: Loss of Condenser
ICF.5.1.02: Partial Loss of Secondary Heat Sink due to Partial Isolation of Steam Route to Condenser
ICF.5.1.03: Turbine Trip

RR SMR PIE
ICF.5.1.04: Steam Generator Isolation due to Spurious Passive Decay Heat Removal
ICF.5.1.06: Spurious Containment Isolation
ICF.5.2.01: Excessive Steam Demand due to Small Isolable Steam Leak
ICF.5.2.02: Excessive Steam Demand due to Small Un-Isolable Steam Leak
ICF.5.3.02: Recoverable Loss of Service Water
LOE.1.0.01: Loss of Offsite Power (72 hours)
LOE.1.0.02: Loss of Offsite Power (168 hours)
LOC.0.1.01: Un-Isolable LOCA (Operator Dose)
LOC.0.2.01: Isolable LOCA (Operator Dose)
LOC.1.1.01: Small Un-Isolable LOCA
LOC.1.2.01: Small Isolable LOCA
LOC.2.1.01: Intermediate Un-Isolable LOCA
LOC.2.1.02: LOCA due to Steam Generator Tube Rupture
LOC.2.1.03: LOCA due to Spurious Reactor Coolant System Relief Valve Lift
LOC.2.1.04: Intermediate Un-Isolable LOCA due to Spurious Primary Blowdown
LOC.2.1.05: Control Rod Drive Mechanism LOCA
LOC.2.2.01: Intermediate Isolable LOCA
LOC.2.2.02: LOCA due to Cold Shutdown Cooling System Heat Exchanger Tube Rupture
LOC.2.2.03: LOCA due to Spurious Opening of Cold Shutdown Cooling System
LOC.3.1.01: Large Un-Isolable LOCA
LOC.3.1.02: LOCA due to Catastrophic Failure in Reactor Pressure Vessel
REF.0.0.01: IC Crane Collision
REF.0.0.02: Spent Fuel Pool Crane Collision
REF.0.0.03: Core Collapse due to Mechanically Unstable Fuel Assemblies
REF.0.0.04: Reactor Core Misload
REF.1.0.01: MOC Bridge / Trolley Collision with an Obstruction on the Rails
REF.1.0.02: MOC Bridge / Trolley Overtravel
REF.1.0.03: MOC Bridge / Trolley Skewing
REF.1.1.01: MOC Main Hoist Double Blocking
REF.1.1.02: MOC Main Hoist Snag and Drag
REF.1.1.03: MOC Main Hoist Restrained Load
REF.1.1.04: MOC Main Hoist Load Path Failure – Non-Arrestable
REF.1.1.05: MOC Main Hoist Load Path Failure – Arrestable

RR SMR PIE
REF.1.1.06: MOC Main Hoist Uncontrolled Lowering
REF.1.1.07: MOC Main Hoist Snag on Raising
REF.1.1.08: MOC Main Hoist Ledge on Lowering
REF.1.1.09: MOC Main Hoist Payload Collision
REF.1.1.10: MOC Main Hoist Over-Raise of Irradiated Components
REF.1.1.11: Inadvertent Withdrawal of one or more Control Rods during Reactor Pressure Vessel Upper Internals Lift
REF.1.2.01: MOC Auxiliary Hoist Restrained Load
REF.1.2.02: MOC Auxiliary Hoist Dropped Load
REF.1.2.03: MOC Auxiliary Hoist Payload Collision
REF.1.2.04: MOC Auxiliary Hoist Over-Raise of Irradiated Item
REF.2.0.01: IC FHM Bridge / Trolley Collison with an Obstruction on Rails
REF.2.0.02: IC FHM Bridge / Trolley Overtravel
REF.2.0.03: IC FHM Bridge / Trolley Skewing
REF.2.1.01: IC FHM Main Hoist Double Blocking
REF.2.1.02: IC FHM Main Hoist Snag and Drag
REF.2.1.03: IC FHM Main Hoist Spurious Grab Disengagement
REF.2.1.04: IC FHM Main Hoist Load Path Failure – Non-Arrestable
REF.2.1.05: IC FHM Main Hoist Load Path Failure – Arrestable
REF.2.1.06: IC FHM Main Hoist Uncontrolled Lowering
REF.2.1.06: IC FHM Main Hoist Uncontrolled Lowering
REF.2.1.07: IC FHM Main Hoist Snag on Raising
REF.2.1.08: IC FHM Main Hoist Ledge on Lowering
REF.2.1.09: IC FHM Main Hoist Mast Seizure
REF.2.1.10: IC FHM Main Hoist Payload Collision with Critical Infrastructure
REF.2.1.11: IC FHM Main Hoist Payload Collision with Upender
REF.2.1.12: IC FHM Main Hoist Over-Raise
REF.2.2.01: IC FHM Auxiliary Hoist Restrained Load
REF.2.2.02: IC FHM Auxiliary Hoist Dropped Load
REF.2.2.03: IC FHM Auxiliary Hoist Collision
REF.2.2.04: IC FHM Auxiliary Hoist Over-Raise of Irradiated Item
REF.3.0.01: SFP FHM Bridge / Trolley Collison with an Obstruction on Rails
REF.3.0.02: SFP FHM Bridge / Trolley Overtravel
REF.3.0.03: SFP FHM Bridge / Trolley Skewing

RR SMR PIE
REF.3.1.01: SFP FHM Main Hoist Double Blocking
REF.3.1.02: SFP FHM Main Hoist Snag and Drag
REF.3.1.03: SFP FHM Main Hoist Spurious Grab Disengagement
REF.3.1.04: SFP FHM Main Hoist Load Path Failure – Non-Arrestable
REF.3.1.05: SFP FHM Main Hoist Load Path Failure – Arrestable
REF.3.1.06: SFP FHM Main Hoist Uncontrolled Lowering
REF.3.1.07: SFP FHM Main Hoist Snag on Raising
REF.3.1.08: SFP FHM Main Hoist Ledge on Lowering
REF.3.1.09: SFP FHM Main Hoist Mast Seizure
REF.3.1.10: SFP FHM Main Hoist Payload Collision with Critical Infrastructure
REF.3.1.11: SFP FHM Main Hoist Payload Collision with Upender
REF.3.1.12: SFP FHM Main Hoist Over-Raise
REF.3.2.01: SFP FHM Auxiliary Hoist Restrained Load
REF.3.2.02: SFP FHM Auxiliary Hoist Dropped Load
REF.3.2.03: SFP FHM Auxiliary Hoist Payload Collision
REF.3.2.04: SFP FHM Auxiliary Hoist Over-Raise of Irradiated Item
REF.4.1.01: Fuel Transfer System (FTS) Structural Failure
REF.4.1.02: FTS Operation during Fuel Loading / Unloading
REF.4.1.03: FTS Carriage Collision with Obstruction
REF.4.1.04: FTS Carriage Overtravel
REF.4.1.05: FTS Spurious Rotation and Travel
REF.4.1.06: FTS Upender Over-Rotation
REF.4.1.07: FTS Carriage Travel with Basket not Horizontal
REF.4.1.08: FTS Fuel Assembly not Seated
REF.4.1.09: FTS Fuel Assembly Falls Out of Basket
REF.4.1.10: FTS Spurious Closure of Sealing Method
REF.4.1.11: FTS Upender Seizure
REF.4.1.12: FTS Upender Rotation with Inadequate Engagement
REF.4.2.01: New Fuel Elevator Structural Failure
REF.4.2.02: New Fuel Elevator Load Path Failure
REF.4.2.03: New Fuel Elevator Basket Seizure
REF.4.2.04: New Fuel Elevator Basket Over-Raise
REF.4.2.05: New Fuel Elevator Basket Raises with Spent Fuel

RR SMR PIE
SFP.1.1.02: Recoverable Loss of Duty Fuel Pool Cooling System
SFP.2.1.01: LOCA in Fuel Pool Cooling System
SFP.2.1.02: Upender Pit Gate Failure
SFP.2.1.03: Cask Loading Pit Gate Failure
SFP.2.1.04: IHP-Lift Gate Failure
SFP.2.2.01: LOCA in Spent Fuel Pool Drain Line
SFP.2.2.02: Cask Gate Failure
SFP.2.2.03: LOCA due to Catastrophic Failure of the Spent Fuel Pool
INT.1.1.01: Fire in Containment
INT.1.1.02: LOCA Conditions in Containment
INT.1.1.03: Minor Disruptive Pipe Failure in Containment
INT.1.1.04: Restrained Disruptive Pipe Failure in Containment
INT.1.1.05: Catastrophic Pipe/Vessel Failure in Containment
INT.1.1.06: Reactor Coolant Pump Disintegration (Missiles)
INT.1.1.07: Valve Stem Missiles in Containment
INT.1.2.01: Fire in the Interspace
INT.1.2.02: Steam Release/Flooding in Interspace
INT.1.2.03: Accumulator Failure
INT.1.2.04: Disruptive Pipe Failure of Main Steam Line
INT.1.2.05: Other Infrequent Internal Hazard in Interspace
INT.1.3.01: Fire in the Fuelling Block
INT.1.3.02: Flooding in the Fuelling Block
INT.1.3.03: Infrequent Hazard in Fuelling Block
INT.1.4.01: Fire in Safety Fluids Block
INT.1.4.02: Flood Originating in Safety Fluids Block
INT.1.4.03: Infrequent Internal Hazard in Safety Fluids Block
INT.1.5.01: Internal Hazard in Safety EC&I Block
INT.1.6.01: Internal Hazard in Auxiliary Block
INT.1.7.01: Internal Hazards in the Main Control Room
INT.2.0.01: Internal Electromagnetic Interference
INT.2.0.02: Hazardous Materials Affecting the Main Control Room
INT.2.1.01: Turbine Disintegration
INT.2.1.02: Other Internal Hazards Outside the Hazard Shield

RR SMR PIE
EXT.0.0.01: Accidental Aircraft Impact
EXT.0.0.02: Storm Including Flooding
EXT.0.0.03: Earthquake
EXT.0.0.04: Tornadic Storm
EXT.0.0.05: Solar Activity
EXT.0.0.06: Cold Weather
EXT.0.0.07: Hot Weather
EXT.0.0.08: Industrial Hazards
NFM.0.0.02: Operator Exposure
NFM.1.1.01: Catastrophic Failure of Liquid Waste Systems
NFM.1.1.02: Uncontained Release from Liquid Waste Systems
NFM.1.1.03: Contained Release from Liquid Waste Systems
NFM.1.1.04: Release from Liquid Retentate System
NFM.1.2.01: Release from Gaseous Waste System
NFM.1.3.01: Release from Solid Waste Storage
NFM.1.3.02: Release from Solid Waste Processing Systems
NFM.1.3.03: Overfill of Solid Waste Storage
NFM.1.3.04: Operator Exposure to Solid Waste Storage
NFM.1.3.05: Operator Exposure to Solid Waste Processing Systems

Abbreviations

AC	Alternating Current
ADS	Automatic Depressurisation System
AFoE	Annual Frequency of Exceedance
ALARP	As Low as Reasonably Practicable
ASD	Atmospheric Steam Dump
ASF	Alternative Shutdown Function
ATWS	Anticipated Transient Without Scram
BAT	Best Available Techniques
BDB	Beyond Design Basis
BEs	Basic Events
BSL	Basic Safety Level
BSO	Basic Safety Objective
BUGS	Back-up Generation System
C&I	Control and Instrumentation
CAE	Claims, Arguments, Evidence
CCF	Common Cause Failures
CCS	Component Cooling System
CCSF	Containment Cooling and Spray Function
CDF	Core Damage Frequency
CDHR	Condenser Decay Heat Removal
CEN	European Committee for Standardization
CET	Core Exit Temperature
CFAST	Consolidated Model of Fire Growth and Smoke Transport
CHF	Critical Heat Flux
CLOF	Complete Loss of Flow
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRM	Control of Radioactive Materials
CRDM	Control Rod Drive Mechanism
CSCS	Cold Shutdown Cooling System
CSM	Containment Safety Measure

CVCS	Chemical and Volume Control System
DB	Design Basis
DBA	Design Basis Analysis
DBC	Design Basis Conditions
DCH	Direct Containment Heating
DDT	Deflagration Detonation Transient
DEC	Design Extension Conditions
DG	Diesel Generator
DiD	Defence-in-Depth
DNB	Departure for Nucleate Boiling
DNBR	Departure for Nucleate Boiling Ratio
DPS	Diverse Protection System
DR	Design Review
DRP	Design Reference Point
DSA	Deterministic Safety Analysis
E3S	Environment, Safety, Security and Safeguards
EBD	Emergency Blow Down
EC&I	Electrical Control and Instrumentation
ECC	Emergency Core Cooling
EMI	Electromagnetic Interference
EMIT	Examination, Maintenance, Inspection and Testing
ESWS	Emergency Service Water System
ET	Event Trees
EUR	European Utility Requirements
FBoM	Functional Bill of Materials
FC	Fractional Contribution
FE	Functional Event
FFT	Functional Fault Tree
FHM	Fuel Handling Machine
FLB	Feed Line Break
FMEA	Failure Modes and Effects Analysis
FPCS	Fuel Pool Cooling System

FSF	Fundamental Safety Functions
FT	Fault Trees
FTS	Fuel Transfer System
FWS	Fire Water System
GB	Great Britain
GDA	Generic Design Assessment
GR	Gate Review
GSE	Generic Site Envelope
HAZOP	Hazard and Operability
HBSC	Human Based Safety Claim
HEAF	High Energy Arcing Fault
HEPs	Human Error Probabilities
HF	Heat Flux
HLSF	High Level Safety Function
HMI	Human-Machine Interface
HPIS	High Pressure Injection System
HPME	High Pressure Melt Ejection
HRA	Human Reliability Assessment
HRS	Hydrogen Reduction System
HTOP	High Temperature Overpressure Protection
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchangers
IAEA	International Atomic Energy Agency
IB LOCA	Intermediate Break Loss of Coolant Accident
ICF	Intact Circuit Faults
IEF	Initiating Event Frequency
IHP	Integrated Head Package
IMS	Integrated Management System
ISO	International Organization for Standardization
IVR	In-Vessel Retention
LBLOCA	Large Break Loss of Coolant Accident

LOC	Loss of Coolant
LOCA	Loss Of Coolant Accidents
LOE	Loss of Electrics
LOOP	Loss Of Offsite Power
LOOW	Loss Of Offsite Water
LRF	Large Release Frequency
LTDHR	Low Temperature Decay Heat Removal
LUHS	Local Ultimate Heat Sink
LWR	Light Water Reactor
MCCI	Molten Corium Concrete Interaction
MCR	Main Control Room
MCSs	Minimal Cut-sets
MCWS	Main Cooling Water System
MKoP	Modularisation Kit of Parts
MOC	Main Overhead Crane
MSIVs	Main Steam Isolation Valves
MSL	Main Steam Line
MSLB	Main Steam Line Break
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
OLCs	Operational Limits and Conditions
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PAR	Passive Autocatalytic Recombiner
PCC	Passive Containment Cooling
PCCS	Passive Core Cooling System
PCSR	Pre-Construction Safety Report
PCT	Peak Clad Temperature
PDHR	Passive Decay Heat Removal
PDS	Plant Damage States

PIE	Postulated Initiating Event
PIRT	Phenomena Identification and Ranking Table
POS	Plant Operating States
PSA	Probabilistic Safety Assessment
PSCS	Passive Steam Condensing System
PWR	Pressurised Water Reactor
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RD	Reference Design
RFI	Radio Frequency Interference
RGP	Relevant Good Practice
RI	Reactor Island
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RR SMR	Rolls-Royce Small Modular Reactor
RVCIS	Reactor Vessel Cavity Injection System
SAA	Severe Accident Analysis
SAD	Severe Accident Depressurisation
SAMG	Severe Accident Management Guidelines
SAPs	Safety Assessment Principles
SBO	Station Black Out
SCR	Supplementary Control Room
SDD	System Design Description
SFP	Spent Fuel Pool
SG	Steam Generator
SGRV	Steam Generator Relief Valve
SGTR	Steam Generator Tube Rupture
SKI	Swedish Nuclear Inspectorate
SMDDs	Safety Measure Design Descriptions
SRVs	Safety Relief Valves
SSC	Structures, Systems and Components
SWIFTs	So-What-If-Techniques

TAG	Technical Assessment Guide
TAM	Test and Assessment Matrix
TBC	To Be Confirmed
TLA	Through Life Activity
TNT	Trinitrotoluene
UK	United Kingdom
UKCP18	UK Climate Projections 2018
US	United States
V&V	Verification & Validation
VHR	Very High Reliability
VTA	Vehicular Transport Accident
VVUQ	Verification, Validation and Uncertainty Quantification
WENRA	Western European Nuclear Regulators Association