Partner Document Number	Partner Document Issue /Revision	Retention category:
n/a	**n/a**	**A**

Title

E3S Case Chapter 15: Safety Analysis

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 Preliminary Concept Definition (PCD) 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 PCD, 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) during operating mode 1 and 2
2. Development of the Fault Schedule and fault sequences for each PIE identified, with specification of safety categorised functional requirements in accordance with the E3S categorisation and classification methodology, with prevention, protection, and mitigation safety measures against all identified fault sequences to deliver their safety functions demonstrating appropriate levels of DiD
3. Preliminary Level 1 and Level 2 Probabilistic Safety Analysis (PSA) has demonstrated that the early design has a Core Damage Frequency (CDF) and Large Release Frequency (LRF) that is significantly below the individual risk and societal risk Basic Safety Objectives (BSOs)
4. Internal Hazards for RR SMR are identified, and the processes that are informing the concept RR SMR design and layout optimisation to inherently minimise internal hazards risk are described
5. 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), with external hazards measures in development including a Hazard Shield and Base Isolation.

Further evidence to support the overall claim and sub-claims will be presented as the E3S Case is progressed alongside the design programme, including: development of the Fault Schedule for all modes of operation, detailed performance analysis to demonstrate safety measures can achieve their safety categorised functional requirements, internal and external hazard analysis and outputs of processes to optimise the design and layout to eliminate or minimise hazards risks, Level 1, 2, and 3 PSA outputs to support the design development and demonstrate risks are below numerical targets, and the outputs of severe accident analyses.

©2023 Rolls-Royce SMR Ltd all rights reserved – copying or distribution without permission is not permitted

Contents

Tables

Figures

15.0 Introduction

15.0.1 Introduction to Chapter

Chapter 15 of the Rolls-Royce Small Modular Reactor (RR SMR) Environment, Safety, Security and Safeguards (E3S) Case forms part of the Pre-Construction Safety Report (PCSR), as defined in E3S Case Chapter 1: Introduction, Reference [1].

Chapter 15 presents the overarching summary and entry point to the safety analysis for the RR SMR, as defined at Reference Design (RD) 5 level of design maturity.

15.0.2 Scope

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, noting DECs are of limited maturity within this revision as detailed below.

The safety analysis will cover all aspects of the RR SMR, including Reactor Island [R01], Turbine Island [T01], Cooling Water Island [C01] and Balance of Plant [B01]. It will cover all modes of operation for the RR SMR, as defined in E3S Case Chapter 13: Conduct of Operations, Reference [2], 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 Chapter 16: Operational Limits & Conditions, Reference [3], and is not covered in this chapter.

Design/Programme Maturity

RR SMR safety analysis presented in this revision of the PCSR is largely based on the design definition at the end of Preliminary Concept Definition (PCD) design stage. PCD is an interim design stage representing RD5 level of design maturity, at which point the status of the safety analysis is broadly:

1. Deterministic Safety Analysis (DSA) predominantly covers Fault Schedule development for Operating Mode 1 and 2 (Power Operations and Start up) and DBCs, with no detailed performance analysis. Other operating modes are presented with reduced maturity

2. Probabilistic Safety Analysis (PSA) includes a limited Level 1 and 2 PSA model based on an RD4 level of design maturity

3. Internal Hazards principles and processes are developed to inform the ongoing design and layout

4. 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)

5. Severe accident analysis is still in development and is therefore not presented in this revision.

The safety analysis is being progressed in line with the design programme to inform the design development and demonstrate that risks are reduced to As Low As Reasonably Practicable (ALARP), see Section 15.0.3.

15.0.3 Claims, Arguments, Evidence Route Map

The Chapter level Claim for E3S Case Chapter 15: Safety Analysis is:

Claim 15: The safety analysis has informed the RR SMR design to provide suitable and sufficient Defence in Depth to deliver the Fundamental Safety Functions, and reduce nuclear safety risks to workers and the public to ALARP

A decomposition of this Claim into Sub-Claims, Arguments, and link to the relevant Tier 2 Evidence is provided in Appendix A. For each lowest level Sub-Claim, the sections of this report providing the Evidence summary are also identified.

The complete suite of evidence to underpin the Claims in the E3S Case will be generated through the RR SMR design and E3S Case programme and documented in the Claims, Arguments, Evidence (CAE) Route Map, Reference [4], described further in E3S Case Chapter 1: Introduction, Reference [1].

15.0.4 Applicable Regulations, Codes & Standards

The RR SMR interpretation of regulations, codes and standards applicable across all areas of E3S are presented in the E3S Design Principles, Reference [5]. Additional codes and standards specifically related to safety analysis include:

1. Published regulatory guidance (e.g., Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs))
2. International Atomic Energy Agency (IAEA) General Safety Guides
3. International Organization for Standardization (ISO)
4. European Committee for Standardization (CEN)
5. Western European Nuclear Regulators' Association (WENRA)
6. European Utility Requirements (EUR).

Additional codes and standards relevant to DSA include:

1. Nuclear Regulatory Commission (NRC) Policy Issue, SECY-93-087

Additional codes and standards relevant to PSA include:

1. IAEA PSA Specific Safety Guides

Additional codes and standards relevant to internal hazards include:

1. IAEA Internal Hazard Specific Safety Guides

Additional codes and standards relevant to external hazards include:

1. Eurocodes

2. United States (US) NRC Regulatory Guides (NUREGs)

15.1Postulated Initiating Events & Fault Sequences

15.1.1 Methodology & Scope

A comprehensive list of all foreseeable Postulated Initiating Events (PIEs) for the RR SMR is essential to show that the design basis and extension conditions within the Fault Schedule are appropriate and follow the Relevant Good Practice (RGP).

A list of PIEs has been developed based on Hazard Identification (HAZID) studies undertaken for the design up to PCD, with outputs from HAZID studies collated and sentenced in the Hazard Log Report, Reference [6], noting this will be continuously updated to capture ongoing HAZID studies across the concept design and as the design matures.

A further review of Operating Experience (OPEX) has been undertaken to ensure the PIE list is comprehensive at this stage of the design, and representative of known and well understood PIEs for existing Pressurised Water Reactors (PWRs). Sources of OPEX include the European Utilities Requirements (EUR), Reference [7], IAEA technical document TECDOC-719, Reference [8] and US NRC NUREG-5750, Reference [9]. Review of other PWR designs will also inform the PIE list as it is developed.

The PIE list is presented in the Definition of PIEs report, Reference [10]. The PIE report includes traceability back to source of the hazard and adopts an appropriate numbering system.

15.1.2 Initiating Event Frequency Derivation

Where possible the Initiating Event Frequency (IEF) for the PIEs has been identified using relevant OPEX. Where OPEX hasn't been available, alternative methods have been used for derivations such as: equipment failure data, predictive human reliability analysis, or a half-tomorrow method (calculation based on the assumption that one event is recorded in double the operating period).

It is noted these methods all have inherent conservatism as generally OPEX and available data from older or generic designs are used as inputs. Further, the design of the RR SMR incorporates sufficient Defence-in-Depth (DiD) and multiple means of achieving the Fundamental Safety Functions (FSFs), providing confidence that any future changes to IEFs, particularly those IEFs that sit near the threshold of a frequent/infrequent fault, can be tolerated within the design.

IEF values are presented in the IEF report, Reference [11]. At PCD, not all PIEs identified have an IEF value derived (see Table 15.1-1), and those available will be reviewed as the design and analysis develop further and revised as necessary.

15.1.3 Grouping of Events

The PIEs identified for RR SMR have been grouped together into the following six categories:

1. Intact Circuit/Plant Faults (ICFs)

2. Loss of Coolant Accidents (LOCAs)

3. Fuel Route & Mechanical Handling

4. Spent Fuel Pool

5. Internal Hazards

6. External Hazards

At PCD, non-fuel melt faults (faults that may lead to a radiological consequence but not a fuel melt scenario) have not been fully considered, though a small number are present in other categories (notably Fuel Route & Mechanical Handling and Spent Fuel Pool). Furthermore, at PCD the focus has been on development of an indicative list of ICFs and LOCAs for Operating Mode 1 and 2 (Power Operations and Start up), noting that PIEs have been identified across all operating modes but the list is not exhaustive. The PIEs will be developed alongside the design programme and reported in future revisions of the PCSR.

15.1.4 Summary of PIEs

Table 15.1-1 summarises all the PIEs that have been identified for the RR SMR up to PCD.

Table 15.1-1: PIEs for RR SMR

PIE ID	**PIE**	**Operating Modes**	**IEF**
Intact Circuit/Plant Faults			
PIE-252	Complete Loss of Pumped Primary Flow	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-253	Partial Loss of Pumped Primary Flow	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-254	Pressure Control System Failure – Heaters Fail On	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-255	Excessive Primary Pressure due to Excessive Operation of Chemistry and Volume Control System (CVCS)	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-256	Primary Pressure Increase due to Pressuriser Spray Valves Failing to Pass Flow	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-258	Primary Pressure Increase due to Failure to Discharge	5A-5B	**{REDACTED FOR PUBLICATION}**
PIE-259	Complete Loss of Steam Generator (SG) Feed	1-4A	**{REDACTED FOR PUBLICATION}**

PIE ID	PIE	Operating Modes	IEF
PIE-260	Complete Loss of Secondary Heat Sink due to Complete Isolation of Steam Route to Condenser	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-261	Complete Loss of Secondary Feed due to Loss of Main Feed Pumps	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-262	Excessive Feedwater Supply	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-263	Complete Loss of Secondary Heat Sink due to Loss of Condenser Vacuum	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-264	Turbine Trip	1	**{REDACTED FOR PUBLICATION}**
PIE-265	Spurious Reactor Shutdown	1-2	**{REDACTED FOR PUBLICATION}**
PIE-266	Complete Loss of Secondary Heat Sink due to Spurious Initiation of Decay Heat Removal (DHR)	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-268	Partial Loss of SG Feed	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-269	Partial Loss of Secondary Heat Sink due to Partial Isolation of Steam Route to Condenser	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-270	Loss of Cold Shutdown Cooling System (CSCS) Heat Sink	4B-6B	**{REDACTED FOR PUBLICATION}**
PIE-271	Primary Pressure Decrease due to Pressuriser Heaters Failing Off	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-273	Excessive Steam Demand due to Small Downstream Steam Leak	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-274	Excessive Steam Demand due to Small Upstream Steam Leak	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-275	Excessive Steam Demand due to Large Downstream Steam Leak	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-276	Excessive Steam Demand due to Large Upstream Steam Leak	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-331	Loss of Off-site Power (LOOP) (2hrs)		**{REDACTED FOR PUBLICATION}**
PIE-332	Loss of Off-site Power (24hrs)		**{REDACTED FOR PUBLICATION}**
PIE-333	Loss of Off-site Power (168hrs)		**{REDACTED FOR PUBLICATION}**

PIE ID	PIE	Operating Modes	IEF
PIE-279	Excessive Control Rod Withdrawal	1-5B	**{REDACTED FOR PUBLICATION}**
PIE-280	Control Rod Ejection	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-281	Significant Power Distribution Imbalance during Critical Operation	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-341	Reactor Coolant Pump Shaft Seizure (Locked Rotor)	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-344	Operator exposure	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-345	Excessive Primary Pressure due to Spurious Initiation of High-Pressure Injection System (HPIS)	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-347	Temperature Reduction of Feedwater Supply	1-4A	**{REDACTED FOR PUBLICATION}**
PIE-348	Primary Pressure Decrease due to Spurious Initiation of Pressuriser Spray	1-5A	**{REDACTED FOR PUBLICATION}**
Loss of Cooling Accidents			
PIE-282	Small un-isolable LOCA in Reactor Coolant System (RCS) or connecting systems	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-283	Small isolable LOCA in RCS or connecting systems	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-284	Intermediate un-isolable LOCA in RCS or connecting systems	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-285	Intermediate isolable LOCA in RCS or connecting systems	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-286	Large un-isolable LOCA in RCS system	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-287	LOCA - catastrophic failure in Reactor Pressure Vessel (RPV)	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-288	LOCA due to excessive discharge	5A-5B	**{REDACTED FOR PUBLICATION}**
PIE-289	LOCA due to spurious reactor circuit relief valve lift	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-290	LOCA due to one SG tube rupture	1-6B	**{REDACTED FOR PUBLICATION}**

PIE ID	PIE	Operating Modes	IEF
PIE-291	Intermediate un-isolable LOCA due to Emergency Core Cooling System (ECCS) injection line leak	*1-5A*	**{REDACTED FOR PUBLICATION}**
PIE-292	Intermediate un-isolable LOCA due to spurious ECCS initiation	1-5A	**{REDACTED FOR PUBLICATION}**
PIE-342	LOCA due to multiple SG tube ruptures	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-346	Containment Bypass LOCA	1-6B	**{REDACTED FOR PUBLICATION}**
External Hazards			
PIE-300	External fire	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-301	External Flood	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-302	Seismic event - Operating Basis Event	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-303	Aircraft Accident Impact	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-1555	Seismic event - Design Basis Event	1-6B	**{REDACTED FOR PUBLICATION}**
Fuel Route & Mechanical Handling			
PIE-304	Uncontrolled Lowering of RPV Head/Internals during a lift	5B-6B	**{REDACTED FOR PUBLICATION}**
PIE-305	Uncontrolled Lowering of a Fuel Assembly during a lift	6A-6B	**{REDACTED FOR PUBLICATION}**
PIE-306	Inadvertent Withdrawal of one or more Control Rods during RPV head lift	5B-6A	**{REDACTED FOR PUBLICATION}**
PIE-307	Incorrect Configuration of Fuel Assemblies	1-2 & 6A-6B	**{REDACTED FOR PUBLICATION}**
PIE-308	Core Collapse due to Physically Unstable Fuel Assemblies	6A-6B	**{REDACTED FOR PUBLICATION}**
PIE-309	Incorrect Storage of Fuel Assemblies in Fuel Rack	6A-6B	**{REDACTED FOR PUBLICATION}**
PIE-310	Small un-isolable LOCA due to structural failure of refuelling cavity boundary or connected system	5B-6B	**{REDACTED FOR PUBLICATION}**

PIE ID	PIE	Operating Modes	IEF
PIE-311	Large un-isolable LOCA due to structural failure of refuelling cavity boundary or connected system	5B-6B	**{REDACTED FOR PUBLICATION}**
PIE-312	Excessive lift of RPV internals due to fuel handling machine failure	5B-6B	**{REDACTED FOR PUBLICATION}**
PIE-313	Excessive lift of fuel assembly due to fuel handling machine failure	6A-6B	**{REDACTED FOR PUBLICATION}**
PIE-314	Loss of refuelling cavity active cooling	6A-6B	**{REDACTED FOR PUBLICATION}**
Spent Fuel Pool			
PIE-337	Loss of Spent Fuel Pool heat sink	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-338	Loss of Spent Fuel Pool systems due to Loss of Offsite Power	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-339	Small LOCA in Spent Fuel Pool	1-6B	**{REDACTED FOR PUBLICATION}**
PIE-340	Large LOCA in Spent Fuel Pool	1-6B	**{REDACTED FOR PUBLICATION}**

15.1.5 List of Internal & External Hazards

The list of Internal and External Hazards applicable to the RR SMR are presented in Section 15.6 and Section 15.7 respectively.

15.1.6 Fault Schedule

The PIEs to be carried forward into the deterministic assessment are analysed in the Fault Schedule, Reference [12]. 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 E3S Case Chapter 3: E3S Objective & Design Rules, Reference [13].

There are several future work items identified for the Fault Schedule, many of which reflect the early stage of the project and the evolving and maturing design, as described in Section 15.0.2. The Fault Schedule will be updated to reflect increased maturity and any changes in the design in line with the CAE Route Map.

15.2 Safety Objectives & Acceptance Criteria

15.2.1 Introduction

The DSA (Section 15.4) will include performance analysis of the fault sequences presented within the Fault Schedule, undertaken in line with the methods outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [13]. Bounding fault and accident sequences are analysed using computer codes to determine performance against justified set of acceptance criteria for RR SMR associated with the relevant the plant state for the fault.

The performance analysis will be carried out using computer codes such as RELAP, VIPER and GOTHIC. Validation of these computer codes alongside the methods, input decks and understanding of error treatment are important aspects of fault studies/ performance analysis. A methods validation strategy and ultimately validation reports will be developed.

At PCD, the performance analysis methodology, including definition of acceptance criteria for each plant state, is still in development in line with the CAE Route Map, and will be reported as the evidence becomes available.

15.3 Human Actions

15.3.1 General Considerations

The safety measures modelled in the DSA (see Section 15.4) encompass both the Systems, Structures, and Components (SSC) delivering the safety function, and any required 'human actions' that the operator needs to take to monitor the initiation and operation of them. Examples of operator actions include:

1. Manual Scram initiation

2. Switch off/on pressuriser heaters

3. Switch off/on CVCS

Operator actions will be systematically assessed through the Allocation of Function (AoF) methodology to determine if they should remain allocated to the operator or if they should be automated, with confirmation that the operator has sufficient and appropriate information, indications and controls available to them to complete the task safely. AoF is an assessment method which aims to assign functions required to meet system goals to an optimised combination of human and engineered elements of the design, described further in E3S Case Chapter 18: Human Factors Engineering, Reference [14].

The Fault Schedule is expected to identify a limited number of operator actions, given the E3S Design Principles dictate that DBC-2ii, DBC-3i, DBC- 3ii and DBC-4 Class 1 and Class 2 safety measures conservatively designed to deliver their functions without reliance on operator action in the Main Control Room (MCR) within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of where actions are required.

Operator actions will also be identified through probabilistic analysis as the PSA model is developed (see Section 15.5).

15.4 Deterministic Safety Analysis

15.4.1 Introduction

The outputs of the DSA presented in this section includes a limited set of PIEs with the following information:

1. Summary of the PIE definition, including IEF and applicable operating modes

2. Fault Schedule extract illustrating the High-Level Safety Function (HLSF), available preventive and protective safety measures and their safety categorisation, aligned to the FSFs of Control of Reactivity and Control of Fuel Temperature (noting measures to achieve Confinement of Radioactive Material are still in development)

3. Qualitative description of the DSA fault sequence

Safety categorised functional requirements are decomposed onto SSC that comprise the safety measures and deliver the HLSFs, which are categorised in accordance with the E3S Categorisation and Classification Methodology, Reference [15].

Performance analysis will be developed to demonstrate that safety measures can achieve their HLSFs and associated acceptance criteria, which will initially be focused on bounding reactor plant ICFs and LOCAs (see Section 15.1.3). Future revisions of this report will also include a summary of this performance analysis evidence, envisaged to include:

1. Discussion of the SSC claimed (or not) as part of the Safety Measure that delivers the HLSF, including supporting systems (Control & Instrumentation (C&I), Heating, Ventilation and Air Conditioning, emergency power supplies etc.)

2. Analysis assumptions for the limiting case, including initial conditions, temperature/pressure range, single failure etc. that inform the development of OLCs

3. Plant state and associated acceptance criteria; as described in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [13], the plant state defines the success criteria that must be met at each level of DiD for protection against each fault. Only Safety Measures that deliver Category A and Category B functionality are credited with reducing sequence frequency required for moving through the DBC-2ii, DBC-3i, DBC-3ii and DBC-4 plant states

4. Performance analysis conclusions and sensitivities

5. Radiological consequence conclusions

The generic aspects of the performance analysis methods and approach will also be described, including the level of conservatism in the approach to ensure sufficient safety margins for each plant state, a description of the computer codes and their verification and validation (V&V), and generic input data.

15.4.2 Analysis of Normal Operation

Normal Operations cover the plant states DBC-1 and DBC-2i. Details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.4.3 Analysis of Design Basis Fault Conditions

This section presents the design basis fault conditions covering plant states DBC-2ii, DBC-3i, DBC-3ii, and DBC-4. At this stage a complete list of PIEs is not available. As such, the PIEs presented below are a sample of the expected fault conditions as developed at PCD, Reference [10]. The full list of PIEs will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

The mechanical SSC that comprise the safety measures outlined below are defined in E3S Case Chapter 6: Engineered Safety Features, Reference [16].

PIE-252: Complete Loss of Pumped Flow

PIE Definition

This hazard is associated with the failure of all Reactor Coolant Pumps (RCPs) causing a complete loss of pumped primary flow. This may be due to mechanical failure such as pump structural failure; electrical failure such as spurious opening of breakers or fuses/relays failing; or operator error.

If unmitigated this would lead to a reduction in the efficacy of the primary heat sink, leading to an increase in fuel temperature, potential fuel melt and consequent radiological release.

This PIE is applicable to modes 1-4A, but not 4B-6B as the RCPs are not needed to provide pumped flow in these modes. The IEF for this fault is **{REDACTED FOR PUBLICATION}** making this an infrequent fault.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	**Preventative Safety Measure**		**First Protective Safety Measure**		**Second Protective Safety Measure**	
	High Level Safety Function	**Category**	**High Level Safety Function**	**Category**	**High Level Safety Function**	**Category**
Control of Reactivity	None	n/a	Scram	A	Alternative Shutdown Function (ASF)	C*
Control of Fuel Temperature	Condenser DHR under Natural Circulation	C	Passive Decay Heat Removal (PDHR)	C*	ECCS	A

* These systems are available to provide a category B function as listed for other faults. However, they are only required as a category C function for this fault in accordance with Reference [15]

Fault Sequence Description

In the event of a loss of pumped flow there is no passive preventative safety measures that are claimed to control reactivity. If this fault is detected Scram will be initiated as a category A safety function, and if this does not provide sufficient reactivity control then the ASF will be enacted to shut down the core as a category C safety function.

In the event of a loss of pumped flow natural circulation will continue to cool the core using the condenser DHR to prevent this becoming a significant event. If this does not provide the temperature control needed, the PDHR will be enacted as a category C protective safety measure. As a final protective measure, the ECCS will activate to flood the core and ensure cooling as the category A protective safety measure.

PIE-259: Complete Loss of SG Feed

PIE Definition

This hazard is associated with the complete loss of secondary feedwater to the SGs. This may be a result of mechanical failure such as feedwater pump failure, drain valve spurious opening, or Feedwater Regulating Valve spurious closure; electrical failure such as spurious signal or loss of electrical supplies to feed pumps; or operator error.

If unmitigated this would lead to a loss of secondary heat sink leading to an inability to remove heat from the core. This will result in increasing core temperature and eventually fuel melt and radiological release.

This PIE is applicable to modes 1-4A, but not 4B-6B because the duty feed and steam system is not in operation during these modes. The IEF for this fault is **{REDACTED FOR PUBLICATION}** making this a frequent fault.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	**Preventative Safety Measure**		**First Protective Safety Measure**		**Second Protective Safety Measure**	
	High Level Safety Function	**Category**	**High Level Safety Function**	**Category**	**High Level Safety Function**	**Category**
Control of Reactivity	None	Not applicable (n/a)	Scram	A	ASF	B
Control of Fuel Temperature	None	n/a	PDHR	B	ECCS	A

Fault Sequence Description

To control reactivity in the core in case of a loss of SG feedwater there are no claimed preventative safety measures. Scram is the category A safety function and acts as the first protective safety measure, with ASF as secondary protective measure and a corresponding category B.

For fuel temperature control there are also no claimed preventative safety measures. The PDHR will form the first protective safety measure with a category B, while the ECCS will be the category A secondary protective safety measure.

PIE-276: Excessive Steam Demand due to Large Upstream Steam Leak

PIE Definition

This hazard is associated with a rupture of the secondary circuit pipework downstream of the last feed line Non-Return Valve (NRV) and upstream of the MSIVs, including stream generator and pipework.

If unmitigated this would lead to a rapid increase in heat removal from the RCS causing excessive core cooling and a corresponding increase in reactivity. This may result in runaway criticality, increasing core temperature, and eventually fuel melt and radiological release.

This PIE is applicable to modes 1-4A, but not 4B-6B because the duty feed and steam system is not in operation during these modes. The IEF for this fault is **{REDACTED FOR PUBLICATION}** making this an infrequent fault.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	Preventative Safety Measure		First Protective Safety Measure		Second Protective Safety Measure	
	High Level Safety Function	Category	High Level Safety Function	Category	High Level Safety Function	Category
Control of Reactivity	None	n/a	Scram	A	ASF	C*
Control of Fuel Temperature	None	n/a	PDHR	C*	ECCS	A

* These systems are available to provide a category B function as listed for other faults. However, they are only required as a category C function for this fault in accordance with Reference [15].

Fault Sequence Description

To control reactivity in the core in case of a large steam leak there are no claimed preventative safety measures as this is not reasonably practicable. Scram is the category A safety function and acts as the first protective safety measure, with ASF as secondary protective measure and a corresponding category C.

As above, for fuel temperature control there are also no claimed preventative safety measures. The PDHR will form the first protective safety measure with a category C, while the ECCS will be the category A secondary protective safety measure.

PIE-280: Control Rod Ejection

PIE Definition

This hazard is associated with mechanical failure of the Control Rod Drive Mechanism (CRDM) via internal pressures in the core forcing the control rod assembly out during normal operation.

Ejection of a control rod will lead to a rapid increase in reactivity which, if unmitigated will result in fuel melt and radiological release. In addition, the ejection may cause a rupture of the core containment leading to a LOCA event which may uncover of the core, resulting fuel melt and the consequent radiological release.

This PIE is applicable to modes 1-5A, but not 5B-6B as there is no pressure differential to drive the control rods out. The IEF for this fault is **{REDACTED FOR PUBLICATION}** making this an infrequent fault.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	**Preventative Safety Measure**		**First Protective Safety Measure**		**Second Protective Safety Measure**	
	High Level Safety Function	**Category**	**High Level Safety Function**	**Category**	**High Level Safety Function**	**Category**
Control of Reactivity	Not reasonably practicable	n/a	Scram	A	ASF	C*
Control of Fuel Temperature	Condenser DHR	C	PDHR	C*	ECCS	A

* These systems are available to provide a category B function as listed for other faults. However they are only required as a category C function for this fault in accordance with Reference [15].

Fault Sequence Description

To control reactivity in the core in case of a control rod ejection it is not reasonably practicable to implement preventative safety measures. Scram is the category A safety function and acts as the first protective safety measure, with ASF as secondary protective measure and a corresponding category C.

For fuel temperature control the condenser DHR acts as a preventative safety measure with a corresponding category C. The PDHR will form the first protective safety measure with a category C, while the ECCS will be the category A secondary protective safety measure.

PIE-286: Large un-isolable LOCA in RCS

PIE Definition

This PIE is related to a loss of primary coolant from the RCS that cannot be isolated from the system, such as leaks in the cold/hot legs of the RCS. The size of this leak is larger than the High-Pressure Injection System (HPIS) or the pressuriser surge link choking size, this is assumed to be equivalent to a full-bore guillotine break of large bore pipework.

If unmitigated a loss of coolant will lead to fuel uncovering in the core and removal of primary heat sink, leading to fuel melt and consequent radiological release. In addition, the failure to properly manage chemistry will lead to pH variation, causing fuel corrosion and structural integrity issues, finally resulting in a radiological release.

This PIE is applicable to modes 1-5B, as modes 6A and 6B relate to refuelling outages where active cooling is not required. The IEF for this fault is **{REDACTED FOR PUBLICATION}**. While this implies a beyond design basis fault, this fault is taken as a design basis infrequent fault in line with RGP.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	**Preventative Safety Measure**		**First Protective Safety Measure**		**Second Protective Safety Measure**	
	High Level Safety Function	**Category**	**High Level Safety Function**	**Category**	**High Level Safety Function**	**Category**
Control of Reactivity	Not reasonably practicable	n/a	Scram	A	Not required	n/a
Control of Fuel Temperature	Not reasonably practicable	n/a	ECCS	A	Not required	n/a

Fault Sequence Description

To control reactivity in the core in case of a large LOCA fault there are no claimed preventative safety measures as they are not reasonably practicable to design. As this is an infrequent fault only one protective safety measure is required, this is Scram as a category A safety function.

Likewise, for fuel temperature control there are no claimed preventative safety measures. The ECCS will form the protective safety measure with a category A.

PIE-290: LOCA due to one SG tube rupture

PIE Definition

This PIE reflects the rupture of one of the steam generator tubes resulting in a loss of primary coolant to the secondary side of the steam generator.

This will cause a loss of primary circuit pressure and primary coolant loss into the secondary circuit. If unmitigated, this loss of coolant may lead to in core boiling, localised heating, fuel melt, and ultimately radiological release.

This PIE is applicable to modes 1-5A, but as the RCS is depressurised in modes 5B-6B this is no longer applicable. The IEF for this fault is **{REDACTED FOR PUBLICATION}** making this a frequent fault.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	**Preventative Safety Measure**		**First Protective Safety Measure**		**Second Protective Safety Measure**	
	High Level Safety Function	**Category**	**High Level Safety Function**	**Category**	**High Level Safety Function**	**Category**
Control of Reactivity	Not reasonably practicable	n/a	Scram	A	ASF	B
Control of Fuel Temperature	Condenser DHR	C	PDHR	B	ECCS	A

Fault Sequence Description

To control reactivity in the core in case of a Steam Generator tube rupture fault there are no claimed preventative safety measures as they are not reasonably practicable to design. Scram provides the primary protective safety measure as the category A safety function, while the ASF provides the secondary safety function with a category B.

For fuel temperature control the condenser DHR provides the preventative safety measures at category C. The PDHR provides a category B primary protective safety function with the ECCS will form the secondary protective safety measure with a category A.

PIE-332: Loss of Offsite Power (24hrs)

PIE Definition

This hazard is a medium-term (between 2 and 24 hours) LOOP fault defined as the loss of all sources of offsite power including the main national grid connection and any auxiliary connections to offsite power sources. Standby and alternative alternating current (AC) power supplies are assumed to remain available.

If power is not restored within reasonable timescales active cooling will not be maintained. This will result in increasing core temperature and fuel uncovering, leading to eventual fuel melt and radiological release.

This PIE is applicable to all operational modes. The IEF for this fault is **{REDACTED FOR PUBLICATION}** making this a frequent fault.

Fault Schedule Extract for Operating Mode 1 and 2

Fundamental Safety Function	Preventative Safety Measure		First Protective Safety Measure		Second Protective Safety Measure	
	High Level Safety Function	Category	High Level Safety Function	Category	High Level Safety Function	Category
Control of Reactivity	TBD	TBD	Scram	A	ASF	B
Control of Fuel Temperature	TBD	TBD	PDHR	B	ECCS	A

Fault Sequence Description

To control reactivity in the core in case of a LOOP fault there are currently no claimed preventative safety measures as the design requires further progression. Scram provides the primary protective safety measure as the category A safety function, while the ASF provides the secondary safety function with a category B.

Likewise, for fuel temperature control there are currently no claimed preventative safety measures. The PDHR provides a category B primary protective safety function with the ECCS will form the secondary protective safety measure with a category A.

15.4.4 Analysis of Design Extension Conditions without Significant Fuel Degradation

Details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.4.5 Analysis of Design Extension Conditions with Core Melt

Details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.4.6 Analysis of Spent Fuel Pool Faults

Details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.4.7 Analysis of Fuel Handling Faults

Details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.4.8 ALARP

On the basis of the preliminary evidence available, there is confidence the design of the RR SMR is on an appropriate trajectory to demonstrate that there will be appropriate DiD provided by the prevention, protection, and mitigation safety measures against all identified fault sequences at this stage to deliver the FSFs.

Performance analysis and assessment of radiological consequences will be undertaken to provide evidence that the safety measures have the capability of achieving their safety functions and meet the defined acceptance criteria with suitable margin. Details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.5 Probabilistic Safety Assessment

15.5.1 Introduction

Maturity Status

The PSA model at PCD is of limited maturity and scope, reflecting design baselines prior to PCD as recorded in Reference [17], including the duty system design baselined in July 2020, the RR SMR safety system design baselined in October 2020, and the outcomes of technical design meetings up to RD4 in April 2021.

A limited set of results for the Level 1 and Level 2 PSA are summarised below, primarily to support the claim that the early RR SMR design can meet numerical targets and achieve a balanced design, with no class of initiating event or design feature making a disproportionate risk contribution.

The PSA model, including methodologies and strategies, are being significantly updated to reflect subsequent design changes. The outputs of the updated PSA will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

Scope

The scope of the PSA at PCD covers ICF and LOCA plant faults during power operations. Operations with the reactor shutdown, refuelling activities, used fuel storage pond and any other site risks are not covered at this stage, nor is assessment of internal and external hazards. Furthermore, dose and consequence modelling in support of a Level 3 PSA has not been undertaken at this stage.

Tools and Input Data

The PSA comprises a linked and integrated event tree and fault tree risk model evaluated using the RiskSpectrum™ software package. The risk model included the following input data:

1. IEFs, Reference [18]
2. Initiating Sequence Diagrams, described in Reference [19]
3. Safety Measure Reliability, Reference [20]

15.5.2 Level 1 PSA Results

Results of the Level 1 PSA evaluation are presented in {REDACTED FOR PUBLICATION Table 15.5-1, based on analysis performed in Reference [17].

{REDACTED FOR PUBLICATION Table 15.5-1: Level 1 PSA Results for Plant Hazards}

15.5.3 Level 2 PSA Results

Level 2 PSA overall Large Release Frequency (LRF) from all reactor plant hazards is calculated as 1.39E-08 per year of power operation, based on analysis performed in Reference [17].

15.5.4 Summary of PSA Insights & ALARP

An overall Core Damage Frequency (CDF) from all reactor plant hazards in the model is identified as 6.19E-08 per year of power operation. This is a factor of 1.6 times smaller than the design target of 1E-07 per year and a factor of 16 times smaller than the BSOs relating to individual risk of the most serious consequences (risk of death, risk of effective dose of >2000mSv).

The calculated CDF and LRF is significantly below the individual risk and societal risk BSOs, and therefore provides confidence that the RR SMR design will achieve the numerical safety targets outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [13].

Analysis of the PSA results identifies that the early RR SMR design is balanced with no single initiating event making a disproportionate CDF contribution. LOCA initiating events collectively are identified to account for 61% of plant fault CDF, with ICFs accounting for 39%. LOCAs of size requiring the ECCS for protection are identified to present the most significant contribution to CDF.

This low CDF reflects the ability of the headline PDHR and ECCS safety measures to deliver their safety functionality entirely passively using natural processes following automatic one-time-movement of a small number of valves to provide the initial alignment. The safety measures are configured with internal redundancy, i.e., multiple trains, such that they are robust to single points of equipment failure and capable of delivering their safety functions with high reliability.

Furthermore, PSA has informed the design up to PCD, with sensitivity studies conducted on various design changes which have supported the changes made and demonstrate that they are contributing to reducing risks to ALARP, these include:

1. Passive depressurisation valves have been incorporated into the baseline ECCS emergency blowdown lines. These reduce the spurious ECCS initiation fault frequency and therefore reducing the predicted CDF

2. Isolation of spurious relief valve lift, which eliminates a demand on ECCS [JN01] for protection, thus reducing the predicted CDF

3. Passive water traps for Local Ultimate Heat Sink (LUHS) breathing. Initial PSA demonstrated common mode failure of LUHS breather valves failure to open on demand (previously required to open during LUHS tank water level lowering, in support of injection to the RCS) as important. Therefore, the functionality provided by the breather valves has been replaced by passive water traps with no mechanical moving parts, providing a significant reliability improvement over breather valves. This has improved the reliability of the ECCS functionality, thus reducing the predicted CDF

4. Surge line NRV low-flow notch, which facilitates a low flow rate of surge into, and out of, the bottom of the pressuriser during normal coolant expansion and contraction transients and as such eliminates several transients, thus reducing the predicted CDF

Overall, the PSA undertaken to date demonstrates that the early RR SMR design, baselined prior to PCD, can meet numerical targets and achieves a balanced design with no class of initiating event or design feature making a disproportionate risk contribution, and confidence that risks can be demonstrably reduced to ALARP.

PSA is also supporting the maturing design with development of a more representative PSA model, providing further PSA insights to inform design, operation, examination, maintenance, inspection, testing (EMIT), emergency planning, safety measures, and qualification requirements. This will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

15.6 Internal Hazards Analysis

15.6.1 Overview

Where practicable, the underpinning safety aim for the RR SMR should be an inherently safe design. Where this is not achievable, the design needs to demonstrate tolerance to hazards, such that if a hazard occurred the design is able to reach a safe state and the risk to nuclear safety is ALARP.

At PCD, input from the internal hazards discipline is required to make informed design decisions which improve the inherent level of safety within the plant and allow the design to progress.

The overall layout of the plant and equipment will be 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. Where limitations of layout are identified, safety measures are required to minimise the impact of faults/ internal hazards.

The safety case for internal hazards is largely built upon segregation i.e., the physical separation of SSC by distance or by means of some form of barrier. The segregation of SSC ensures that individual losses of equipment can be tolerated within the safety case due to redundant equipment remaining available.

E3S design principles and requirements have been identified to inform the layout, which includes principles relevant to internal hazards presented in Reference [5]. Internal hazards specialist support is also provided to the layout and design teams to eliminate or minimise the impact of internal hazards.

15.6.2 Approach

The identification and the characterization of internal hazards should include a consideration of the initial conditions, the magnitude and the likelihood of the hazards, the locations of the sources of the hazards, the resulting environmental conditions, and the possible impacts on SSC important to safety or on other SSC.

Internal hazard assessments considers whether a PIE occurs due to a hazard, and whether the hazard can also damage the claimed safety measures for that PIE. Each hazard sequence will be analysed to define the consequences (and may refer to IEFs defined in the DSA). Further assessments may be required from design teams and/or the external hazards team to understand the sequences and magnitude of hazards.

PIEs will then be included in the Fault Schedule and DSA will be used to define hazard protection requirements to ensure there are sufficient and suitable safety measures available (e.g., requirements placed on divisional barriers, pipe whip restraints, shields, or on withstand of SSC comprising the safety measures). Hazard protection measures will be classified, and safety categorised functional requirements will be defined for input to design substantiation.

Figure 15.6-1 provides a generic flow diagram of the internal hazard approach.

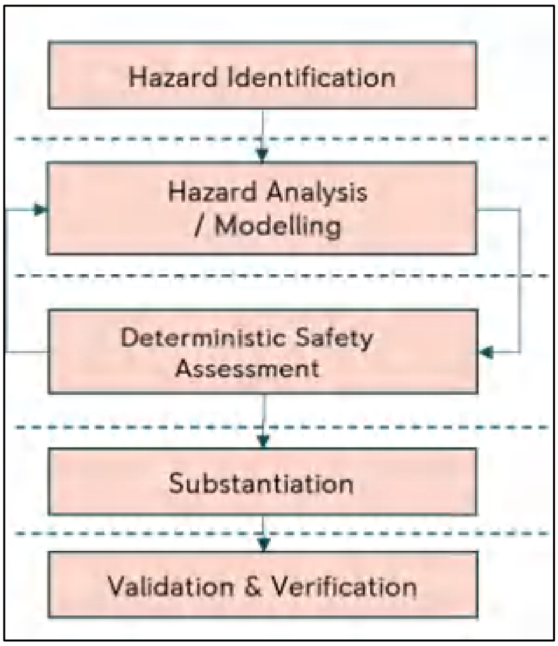

Figure 15.6-1: Internal Hazard Approach Flow Diagram

15.6.3 List of Internal Hazards

Individual Hazards

The individual internal hazards for RR SMR and their definitions, Reference [21] have been listed in Table 15.6-1. The list of internal hazard types is not exhaustive but intended to support the specific assessments that will follow as the design progresses.

Table 15.6-1: List of individual Hazards and Definitions

Individual Hazard	**Definition**
Fire	The internal fire hazards considered are: • Building/solid material fires • 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.

Individual Hazard	Definition
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 overpressurisation 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 are: • 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 loads (due to unplanned crane movements, crane failures or local support failures) are also usually considered as part of this topic

Individual Hazard	Definition
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 are: • Gas cylinders (e.g., nitrogen) • Atmospheric storge tanks (e.g., hydrazine hydrate) • Batteries (e.g., sulphuric acid)
Vehicular Transport Accidents (VTA)	Assessment of vehicle impact hazards on plant equipment or structures. This hazard requires some knowledge of items which are usually plant specific.

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:

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

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

3. 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 >10E-7/year

The RR SMR will also demonstrate plant resilience to external-internal hazard combinations.

15.6.4 Design Approach

Layout Optimisation

Layout reviews and hazard identification is being undertaken early in the design process and throughout design development to ensure the layout is optimised to eliminate or minimise the impact of internal hazards. The internal hazards process for optimisation of the layout is summarised in Figure 15.6-2.

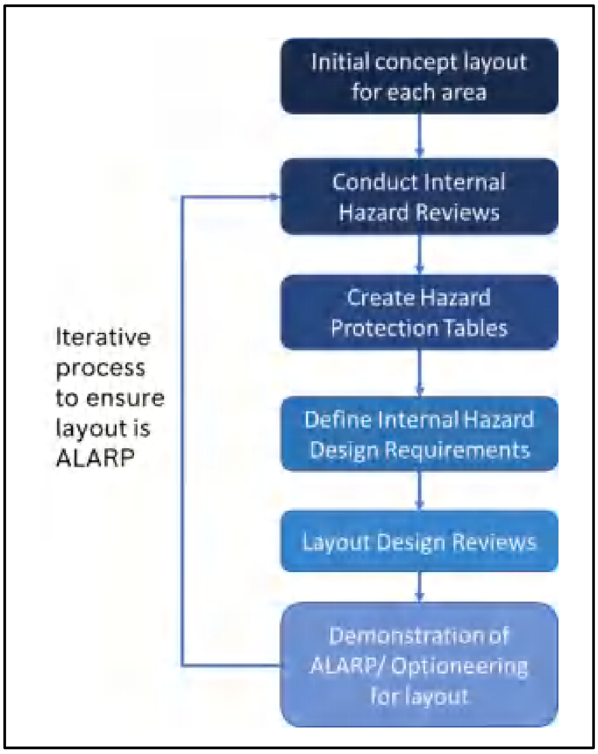

Figure 15.6-2: Internal Hazards Process for Layout Optimisation

A summary of the outputs of this process will be presented in a future revision of the E3S Case as the layout for the concept design is finalised.

Design Guidance

As part of the internal hazards' specialist support to the layout and design, a set of design considerations has been developed to provide guidance to designers in the development of a safe by design approach in relation to internal hazards. Examples are provided below (noting this is not exhaustive):

1. Fire: minimisation of fire loads and ignition sources, design of building structures to be fire resistant
2. Explosion: elimination by design where practicable, limiting the formation of explosive atmospheres, locating oil tanks away from buildings containing SSC
3. Flooding: segregation of water source away from SSC where practicable, provision of leak detection or isolation systems
4. Pipe Whip: design of SSC to withstand the effects of pipe failures, appropriate restraint design
5. Steam Release: minimisation of steam sources, direct steam via an engineered route to open air via vents
6. Missiles: design of vessels and valves etc. such that they cannot become a missile, no single failure should lead to generation of a missile
7. Blast: suitable blast wave venting, locating blast sources away from SSC, blast walls

8. EMI: redundancy, diversity and segregation to reduce pervasiveness of EMI, physical controls such as EMI detection devices or exclusion zones for potential EMI sources

9. Dropped Loads: fuel handling and lift routes to avoid potential drops on SSC, scheduling of load movements in specific modes of plant operation

10. Hazardous Materials: storage away from personnel, minimisation of quantities in storage, appropriate ventilation

11. VTA: provision of energy absorbing barriers, zonal restrictions

15.6.5 Analysis

A proportionate approach will be applied to the internal hazards assessment depending on fault/building type, the significance of the consequences of hazards and the class of safety systems affected. The level of assessment applied to hazards is dependent on the frequency of that hazard.

The suitability and sufficiency of safety measures for internal hazards is considered both through DSA and by meeting RGP. The latter may inform the DSA e.g., by identifying safety measures and associated SSC, or may identify additional DiD measures for preventing and protecting against hazards to ensure the risks have been reduced to ALARP.

Internal hazard analysis will be focused on buildings:

1. Containing SSC that deliver safety functions relating to reactor trip and post trip cooling, or containing essential support equipment supporting these functions

2. Containing radiological inventories

3. Operational/running plants whose failure could lead to a demand on safety systems, e.g. connection to ultimate heat sink

4. Containing potential, credible hazard sources which could threaten SSC or radiological inventories in other buildings

The internal hazards strategy and methodologies for analysis of bounding internal hazards cases, and the outputs of analysis, will be presented in a future revision of the E3S Case as evidence in the CAE Route Map is developed.

15.7 External Hazards Analysis

15.7.1 Overview

In addition to plant faults, RR SMR considers external hazards in the context of nuclear safety, i.e., hazards arising from outside the bounds of the power station that are considered as PIEs that could challenge the delivery of the FSFs. External hazards are defined as 'natural or man-made hazards to a site and facilities that originate externally to both the site and its processes'.

At PCD, 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 Chapter 2: Generic Site Characteristics, Reference [22], 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 it is capable of being built and operated in a way that is safe, secure, and tolerant to external hazards.

Comprehensive analysis 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 developed in line with the CAE Route Map.

15.7.2 List of External Hazards

Development Process

A complete list of potential external hazards for RR SMR was first produced in Reference [23], based on a review of internal sources, RGP, United Kingdom (UK) Regulatory Guidance and international documentation including:

1. RR SMR Hazard Log, Reference [6]

2. ONR Guidance:

a. ONR SAPs, Reference [24]

b. ONR Technical Assessment Guide (TAG) 13, Reference [25]

3. WENRA guidance on new Nuclear Power Plant Design, Reference [26] and

4. US NRC guidance on external hazards and Probabilistic Safety Assessment (PSA), References [27] and [28].

A secondary review was carried out in Reference [29], which examined the following additional guidance:

1. Requirements produced by the EUR Organisation for new large and mid-sized Nuclear Power Plants, Reference [30]

2. Swedish Nuclear Inspectorate (SKI) Guidance on external hazards, Reference [31]

3. European Commission guidance on external hazards, Reference [32]

4. Organisation for Economic Co-operation and Development (OECD) guidance on external hazards, Reference [33]

5. IAEA Safety Standard NS-G-1.5, Reference [34]

As part of the GSE development, a further review of previous Generic Design Assessment (GDA) submissions has been undertaken, to produce a final list of unscreened hazards, presented in Reference [35].

Screening Criteria

The superset of unscreened hazards has been screened to those relevant to the RR SMR using the following criteria:

1. Low frequency: judged that the hazard frequency for a GB site is less than 10E-7/yr

2. Low consequence: judged that the hazard would have no significant identified consequential effect on the safety of the facility

3. Covered elsewhere: the hazard is covered by another hazard such that they can be grouped together

Additionally, several hazards are screened in for consideration, however judged to be site specific and therefore will not be subject to significant assessment during GDA.

External Hazard List

The list of external hazards that have been screened for the generic RR SMR design includes:

1. Air temperature

2. Relative humidity

3. Wind

4. Tornado

5. Tornadic missiles

6. Rainfall

7. Hail, sleet and snow

8. Ice

9. Cooling water temperature

10. Lightning

There are also several external hazards that have site specific elements, for which the GSE provides commentary, including:

1. Seismic
2. Accidental aircraft crash
3. Landscape changes
4. Space weather
5. Flooding
6. Drought
7. Industrial
8. Biological

The GSE provides consideration for addressing these hazards in the design, e.g., civils design of the aseismic bearing is informed by seismic response spectra specified in the GSE, and the hazard shield withstand design is informed by aircraft impact load functions.

Identification and assessment of site-specific hazards shall be undertaken at the site licensing and permissioning stages by the future dutyholder/licensee. 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 in the following Commitment:

Commitment on Future Dutyholder/Licensee C15.1: The future dutyholder/licensee shall identify all site-specific external hazards and provide a suitable safety justification

External Hazards Combinations

Hazard combinations will also be developed and considered for RR SMR, noting they have not yet been identified. This will include:

1. Consequential Hazards: One or more hazards that affect the plant and occur as the result of a separate event that also affects the plant. For example, rainfall could lead to external flooding

2. Correlated Hazards: One or more hazards that affect the plant in the same time frame due to persistence or similar causal factors. For example, an external explosion could lead to external fire and external missiles occurring simultaneously

3. Independent (Coincidental) Hazards: Combinations of randomly occurring independent events affecting the plant simultaneously. For example, seismic activity and high air temperature are not causally related

To identify all possible credible combinations of external hazards, the methodology will involve the following steps:

1. Define several credible scenarios, identifying the primary and consequential hazards

2. Prepare a matrix of external hazards to identify all combinations

3. Identify those combinations included in the scenarios

4. Review remaining combinations to determine relationship (consequential, correlated, or independent)

5. Review matrix to determine if additional scenarios should be highlighted

6. Present results in a matrix

The methodology for consideration of combinations of hazards is in development and will be reported in a future revision of the E3S Case in line with the CAE Route Map.

15.7.3 Design Development for External Hazards

The RR SMR is developing the following measures to deliver safety functions that protect against external hazards:

1. Hazard Shield: a reinforced structure surrounding the Containment, Fuelling Building (including Spent Fuel Pool), and the Safeguards Block (Main Control Room (MCR) and associated critical systems – fluids and C&I) in Reactor Island [R01]. The structure is being designed to withstand a bounding aircraft impact, aiming to provide protection to Class 1 and 2 SSC

2. Base Isolation: the installation of horizontally flexible and vertically stiff seismic isolators between structures in Reactor Island [R01] and the substructure aseismic bearings, decoupling the structures from ground motion during a design basis earthquake seismic spectra anchored to a peak ground acceleration (PGA) of 0.3g, for both vertical and horizontal spectra, for hard, medium, and soft sites. The structures in Reactor Island [R01] currently located on the Base Isolation are those within the Hazard Shield, aiming to protect Class 1 and 2 SSC, which will be seismically qualified as required

Further information on the design of the Hazard Shield and Base Isolation at PCD is described in E3S Case Chapter 9B: Civil Engineering Works & Structures, Reference [36].

15.7.4 Analysis of External Hazards & ALARP

Analysis of external hazards to support the demonstration of ALARP will be reported in a future revision of the E3S Case as evidence in the CAE Route Map is developed.

15.8 Conclusions

15.8.1 Conclusions

Preliminary evidence is presented to support the overall chapter claim that 'The safety analysis has informed the RR SMR design to provide suitable and sufficient levels of DiD to deliver the FSF and reduce nuclear safety risks to workers and the public to ALARP', which contributes to the overall E3S objective to protect people and the environment from harm, and the demonstration that risks are reduced ALARP.

The methodology for establishing a comprehensive list of PIEs and respective IEFs is presented, using inputs from HAZID studies of the RR SMR design and relevant OPEX and RGP. The list of PIEs developed for PCD focuses on ICFs and LOCAs applicable to operational mode 1 and 2. Further operational modes and categories of faults will be developed as the design maturity increases.

DSA presents the HLSFs and the available preventative and protective safety measures that deliver them for design basis fault conditions. The HLSFs presented are aligned to the FSFs of 'Control of Reactivity' and 'Control of Fuel Temperature'. As design maturity increases normal operation conditions and design extension conditions will be considered, as well as safety measures to achieve the FSF 'Confinement of Radioactive Material'.

The methodologies for performance analysis and the derivation of human actions within DSA are under development and will be reported in a future revision of the E3S Case. Performance analysis and assessment of radiological consequences is also in development, which will provide evidence that the safety measures have the capability of achieving their safety functions and can meet the defined acceptance criteria with suitable margin.

PSA modelling of the early design demonstrates a CDF from all reactor plant hazards that is significantly below the individual risk and societal risk Basic Safety Objectives (BSOs). This provides confidence that the RR SMR design can achieve the numerical safety targets required for the E3S case. A detailed PSA for the maturing design is in development.

The strategy and principles for internal hazards are informing the concept design and layout of the RR SMR to provide tolerance to anticipated hazards. Evidence of the internal hazards informed design, internal hazards methodologies and analysis of bounding internal hazards cases is in development.

External hazards applicable to the RR SMR generic design have been identified and screened. External hazards values have been derived and justified in the GSE to inform the design of hazard protection measures being developed for RR SMR, including the Hazard Shield and the Base Isolation. Methodologies for external hazards analysis are also in development, including combinations of hazards.

The full suite of evidence to underpin the claim is in development in line with the CAE Route Map and will be reported in future revisions of the E3S Case.

15.8.2 Assumptions & Commitments on Future Dutyholder/Licensee

Table 15.8-1: Assumptions & Commitments on Future Dutyholder/Licensee

ID	Description
C15.1	The future dutyholder/licensee shall identify all site-specific external hazards and provide a suitable safety justification

15.9 References

[1] RR SMR Report, SMR0004294/001, “E3S Case Chapter 1: Introduction,” March 2023.

[2] RR SMR Report, SMR0004247/001, “E3S Case Chapter 13: Conduct of Operations,” March 2023.

[3] RR SMR Report, SMR0004555/001, “E3S Case Chapter 16: Operational Limits & Conditions,” March 2023.

[4] RR SMR Report, SMR0002155/001, “E3S Case Route Map,” March 2023.

[5] RR SMR Report, SMR0001603/001, “Environmental, Safety, Security and Safeguarding Design Principles,” August 2022.

[6] RR SMR Report, SMR0001317/004, “Hazard Log Report,” October 2022.

[7] EUR, “Generic Nuclear Island Requirement: Chapter 1 Safety Requirements (Volume 2), Rev. E,” 2016.

[8] IAEA, “Defining initiating events for purposes of probabilistic safety assessment (TECDOC-719),” 1993.

[9] J. P. Poloski et al, “Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995 (NUREG/CR-5750),” 1998.

[10] RR SMR Report, SMR0001389/001, “Definition of Postulated Initating Events,” October 2022.

[11] RR SMR Report, SMR0001393/001, “Review of Initiating Event Frequencies of Postulated Initiating Events,” October 2022.

[12] RR SMR Report, EDNS01000470763/005, “Fault Schedule Report,” September 2021.

[13] RR SMR Report, SMR0004589/001, “E3S Case Chapter 3: E3S Objectives & Design Rules,” March 2023.

[14] RR SMR Report, SMR0004520, “E3S Case Chapter 18: Human Factors Engineering,” March 2023.

[15] RR SMR Report, EDNS01000887611/001, “Environment, Safety, Security and Safeguards Categorisation and Classification Method,” May 2020.

[16] RR SMR Report, SMR0003771/001, “E3S Case Chapter 6: Engineered Safety Features,” March 2023.

[17] RR SMR Report, EDNS01000966510/001, “PSA Risk Spectrum model V1.0 reflecting the design as baselined at Decision 21 and Decision 22,” May 2021.

[18] RR SMR Report, EDNS01000475198/001, “Initiating Fault Cause Frequencies for SMR Plant Hazards,” September 2016.

[19] RR SMR Report, EDNS01000537027/001, “SMR Probabilistic Safety Assessment,” March 2021.

[20] RR SMR report, EDNS01000537023/001, “Safety Measure Reliability Report,” March 2017.

[21] RR SMR Report, EDNS01000926210/001, “Internal Hazards Strategy & Safety Case Requirements,” November 2020.

[22] RR SMR Report, SMR0004542/001, “E3S Case Chapter 2: Generic Site Characteristics,” March 2023.

[23] RR SMR Report, EDNS01000475199/002, “Definition of Design Basis for Internal/External Hazards,” 2017.

[24] ONR, “Safety Assessment Principles for Nuclear Facilities, Revision 1,” 2020.

[25] ONR NS-TAST-GD-013, “Nuclear Safety Technical Assessment Guide 13: External Hazards, Revision 8.1,” December 2022.

[26] WANO, “Safety of New NPP designs. Study by Reactor Harmonization Working Group RHWG,” March 2013.

[27] US NRC, NUREG-1407, “Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities,” June 1991.

[28] US NRC, “NUREG/CR-2300 A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,” 1983.

[29] RR SMR Report, EDNS01000965477/001, “External Hazards Review,” May 2021.

[30] EUR, “European Utility Requirements LWR Nuclear Power Plants Volume 2 Generic Nuclear Island Requirements, Chapter 4: Design Basis, Revision E,” October 2016.

[31] SKI, “ISSN 1104–1374, ISRN SKI-R-02/27-SEGuidance for External Events Analysis, 02:27,” February 2003.

[32] 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.

[33] OECD-NEA, “Probabilistic Safety Analysis (PSA) of Other External Events than Earthquake, NEA/CSNI/R(2009),” March 2009.

[34] IAEA, NS-G-1.5, “External Events Excluding Earthquakes in the Design of Nuclear Power Plants,” November 2003.

[35] RR SMR Report, SMR0001535/001, “RR SMR UK Generic Site Envelope,” August 2022.

[36] RR SMR Report, SMR0003778/001, “E3S Case Chapter 9B: Civil Engineering Works & Structures,” March 2023.

15.10 Appendix A: CAE Route Map

15.10.1 Chapter 15 Route Map

A preliminary Claims decomposition from the overall Chapter 15 Claim is summarised in Table 15.10-1, including the Tier 2 Evidence supporting the Claim (at this revision), and section of this report where the Evidence is summarised.

Table 15.10-1: CAE Route Map

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 15**	**Underpinning Tier 2 Evidence** **at PCD*	**Underpinning Tier 2 Evidence** **to be developed*
All credible PIEs for the RR SMR design are identified, fully defined, and sentenced appropriately for analysis	-	-	-	Section 15.2	Definition of PIEs Report, Reference [10] Derivation of IEFs Report, Reference [11]	Definition of PIEs Report (revised, to also include IEF derivation)
For all PIEs, the FSF are delivered across all levels of DiD by Safety Measures which deliver categorised High Level Safety Functions	HLSFs are identified for each PIE at each level of DiD, aligned to each Fundamental Safety Function	-	-	Section 15.5	Fault Schedule, Reference [12]	Fault Schedule (revised to reflect increasing design maturity)

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 15**	**Underpinning Tier 2 Evidence** **at PCD*	**Underpinning Tier 2 Evidence** **to be developed*
	HLSFs are linked to Safety Measures and assigned a safety category in line with Categorisation & Classification methodology	-	-	n/a	n/a	Safety Measures Dynamic Object-Oriented Requirements System (DOORS) Module
	Safety categorised functional requirements are placed on SSC that comprise Safety Measures delivering the HLSFs, with SSC classified according to the categorisation of the functional requirements they deliver	-	-	n/a	n/a	DOORS database – safety modules linked to various design modules

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 15**	**Underpinning Tier 2 Evidence** **at PCD*	**Underpinning Tier 2 Evidence** **to be developed*
Deterministic analysis approach is defined and justified with appropriate conservatism	Acceptance Criteria for Performance Analysis are defined and justified with suitable margin	-	-	Section 15.3	n/a	Design Basis Performance Analysis Methodology Severe Accident Analysis Methodology
	Computer codes and models used for deterministic performance analysis are validated	-	-	Section 15.5.1	n/a	Thermal Hydraulics V&V Summary
Deterministic analysis of normal and abnormal operation conditions (plant states DBC-1 and DBC-2i) identified in the Fault Schedule demonstrates that all relevant acceptance criteria are met	-	-	-	Section 15.5.2	n/a	Fault Analysis Summary Report – Reactor Plant

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 15**	**Underpinning Tier 2 Evidence** **at PCD*	**Underpinning Tier 2 Evidence** **to be developed*
Deterministic analysis of design basis fault conditions (plant states DBC-2ii/3i/3ii/4) identified in the Fault Schedule demonstrates that all relevant acceptance criteria are met	-	-	-	Section 15.5.3	n/a	Fault Analysis Summary Report – Reactor Plant
Deterministic analysis of design extension conditions without fuel degradation (plant state DEC-A) identified in the Fault Schedule demonstrates that all relevant acceptance criteria are met and the absence of "cliff-edge" effects for beyond Design Basis events	-	-	-	Section 15.5.4	n/a	Severe Accident Analysis Summary Report

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 15	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
Severe accident analysis of design extension conditions with core melt (plant state DEC-B) demonstrates that all relevant acceptance criteria are met	-	-	-	Section 15.5.5	n/a	Severe Accident Analysis Summary Report
Deterministic analysis of spent fuel pool faults (plant state DBC-1 to DEC-A demonstrates that all relevant acceptance criteria are met	-	-	-	Section 15.5.6	n/a	Fault Analysis Report – Spent Fuel Pool

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 15	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
Deterministic analysis of Fuel Handling faults (plant state DBC-1 to DEC-B) identified in the Fault Schedule demonstrates that all relevant acceptance criteria are met	-	-	-	Section 15.5.7	n/a	TBC
RR SMR is tolerant to all credible low frequency external hazards (including combinations of hazards/Fukushima type events) and all acceptance criteria are met	-	-	-	n/a	n/a	Severe Accident Analysis Summary Report
The Operating Assumptions, Limits & Conditions set by the Performance Analysis are incorporated into Operating Technical Specifications	-	-	-	n/a	n/a	TBC

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 15**	**Underpinning Tier 2 Evidence** **at PCD*	**Underpinning Tier 2 Evidence** **to be developed*
The Operating Assumptions in the Severe Accident Management Strategy which are used in the analysis are correctly captured in operational procedures	-	-	-	n/a	n/a	TBC
RR SMR is tolerant to all Internal Hazards (including Combined Hazards)	All credible initiating events for Internal Hazards are identified and sentenced for analysis	-	-	Section 15.7.3	n/a	Internal Hazards Strategy
	The layout and design of the RR SMR is optimised to eliminate or minimise the impact of internal hazards	-	Design processes for layout optimisation and design guidelines inform the early design development	Section 15.7.4	n/a	Internal Hazards Summary Reports (Inside and Outside Hazard Shield)
	TBC	-	-	-	-	-

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 15	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
RR SMR is tolerant to all External Hazards (including Combined Hazards)	All credible initiating events for External Hazards are identified and sentenced for analysis	-	External hazards have been derived and screened using UK and international RGP and OPEX	Section 15.8.2	GB GSE Report	Global GSE Report
	TBC	-	-	-	-	-
The probabilistic safety assessment demonstrates that nuclear safety risks to workers and the public are understood and acceptable and is used appropriately throughout the plant lifecycle	The probabilistic safety assessment is suitable and sufficient to support nuclear safety	-	-	Section 15.6.1	IEFs, Reference [18] Initiating Sequence Diagrams, Reference [19] Safety Measure Reliability, Reference [20]	PSA Technical Requirements PSA Development Strategy
	The probabilistic safety assessment is used appropriately to support nuclear safety throughout the plant lifecycle	-	-	Section 15.6.2, 15.6.3, 15.6.4	RR SMR PSA Risk Spectrum Model V1.0, Reference [17]	TBC

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 15	Underpinning Tier 2 Evidence **at PCD*	Underpinning Tier 2 Evidence **to be developed*
	The probabilistic safety assessment demonstrates that radiological risks are acceptable	-	-	Section 15.6.2, 15.6.3, 15.6.4	RR SMR PSA Risk Spectrum Model V1.0, Reference [17]	PSA Main Report

15.11 Acronyms and Abbreviations

AC	Alternating Current
ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
ASF	Alternative Shutdown Function
BSO	Basic Safety Objective
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CDF	Core Damage Frequency
CEN	European Committee for Standardisation
CRDM	Control Rod Drive Mechanism
CSCS	Cold Shutdown Cooling System
CVCS	Chemistry and Volume Control System
DBC	Design Basis Condition
DEC	Design Extension Condition
DHR	Decay Heat Removal
DiD	Defence-In-Depth
DOORS	Dynamic Object-Oriented Requirements System
DSA	Deterministic Safety Analysis
E3S	Environment, Safety, Security and Safeguards
ECCS	Emergency Core Cooling System
EMI	Electromagnetic Interference
EMIT	Examination, Maintenance, Inspection, and Testing
EUR	European Utility Requirements
FSF	Fundamental Safety Function
GB	Great Britain
GDA	Generic Design Assessment
GSE	Generic Site Envelope

HAZID	Hazard Identification
HEAF	High Energy Arcing Faults
HLSF	High-Level Safety Function
HPIS	High-Pressure Injection System
IAEA	International Atomic Energy Agency
ICF	Intact Circuit Fault
IEF	Initiating Event Frequency
ISO	International Organization for Standardization
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Off-site Power
LRF	Large Release Frequency
LUHS	Local Ultimate Heat Sink
MCR	Main Control Room
n/a	Not Applicable
NRC	Nuclear Regulatory Commission
NRV	Non-Return Valve
NUREG	(US) Nuclear Regulatory Commission
OECD	Organisation For Economic Co-Operation and Development
OLC	Operational Limit and Condition
ONR	Office for Nuclear Regulation
OPEX	Operating Experience
PCD	Preliminary Concept Definition
PCSR	Pre-Construction Safety Report
PDHR	Passive Decay Heat Removal
PGA	Peak Ground Acceleration
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor

RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RD	Reference Design
RGP	Relevant Good Practice
RFI	Radio Frequency Interference
RPV	Reactor Pressure Vessel
RR	Rolls-Royce
SAP	Safety Assessment Principle
SG	Steam Generators
SKI	Swedish Nuclear Inspectorate
SMR	Small Modular Reactor
SSC	System, Structure, and Component
TAG	Technical Assessment Guide
TECHDOC	Technical Document
UK	United Kingdom
US	United States
V&V	Verification and Validation
VTA	Vehicular Transport Accidents
WENRA	Western European Nuclear Regulators' Association