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

Title

E3S Case Chapter 6: Engineered Safety Features

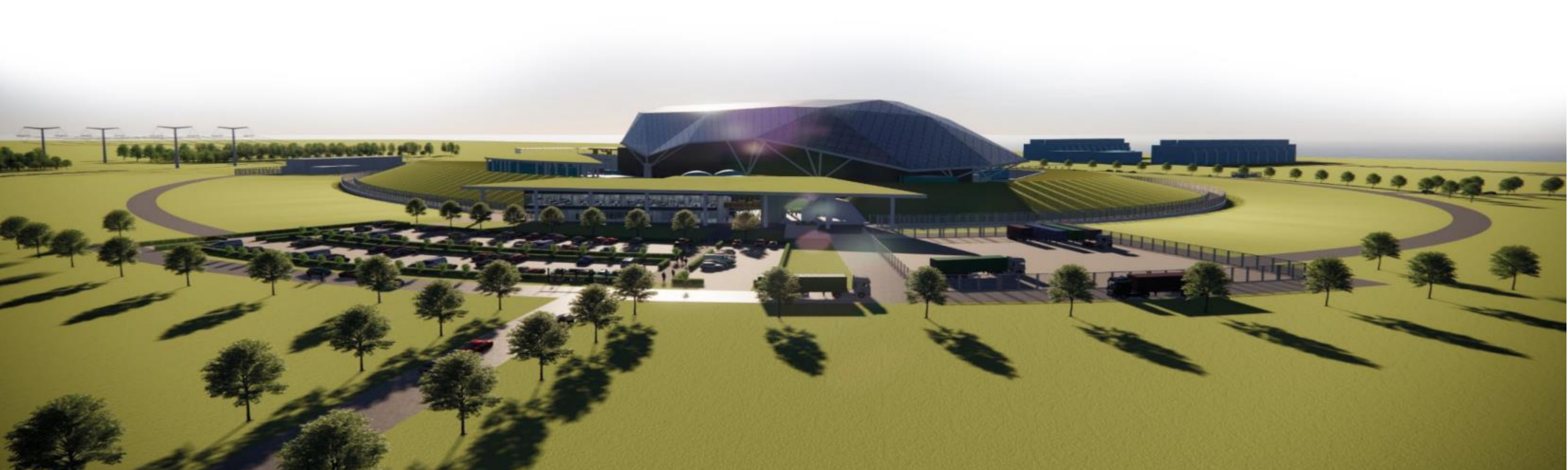
Executive Summary

This chapter of the Environment, Safety, Security, and Safeguards (E3S) Case presents the Engineered Safety Features of the Rolls-Royce Small Modular Reactor (RR SMR). It outlines the arguments and preliminary evidence available at the Preliminary Concept Definition (PCD) design stage to underpin the high-level Claim that the RR SMR Engineered Safety Features are designed and substantiated to achieve functional and non-functional safety requirements through the lifecycle, and reduce risks to As Low As Reasonably Practicable (ALARP).

The Engineered Safety Features include the Structures, Systems and Components (SSCs) that deliver the safety functions during design basis fault conditions and design extension conditions. The SSCs summarised in this revision of the E3S Case include the Emergency Core Cooling System (ECCS) [JN01], Passive Decay Heat Removal System (PDHR) [JN02], Scram [JD01], Alternative Shutdown Function (ASF) [JD02], and Containment Vessel [JMA].

For each SSC, the safety categorised functional requirements, non-functional system requirements, and design description are summarised based on the maturity level at PCD. The key verification activities to substantiate the requirements are also described.

The full suite of evidence to underpin the Claim is still in development, including full traceability of safety categorised requirements from the safety analysis, a complete set of non-functional system requirements from the E3S design principles, further development of the SSC concept design to meet safety requirements, and ultimately substantiation of safety requirements.



Contents

Tables

Figures

6.0 Introduction

6.0.1 Introduction

Chapter 6 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 6 presents the overarching summary and entry point to the design information for the Structures, Systems and Components (SSCs) that deliver the safety functions during Design Basis Conditions (DBCs) (fault conditions) and Design Extension Conditions (DECs), as defined at Reference Design (RD) 5 level of design maturity.

6.0.2 Scope

The list of SSCs that are included in the scope of this chapter is provided in Section 6.10, Appendix B, including those that are within scope but excluded from this revision due to design immaturity. The scope covers SSCs that deliver safety functions at Defence-in-Depth (DiD) levels 3 and 4 (see E3S Case Chapter 3: E3S Objectives and Design Rules, Reference [2], for further details on DiD levels).

For each SSC in scope, the following aspects are broadly summarised:

1. Fundamental Safety Functions (FSFs) delivered by the SSC, and the assigned categorised functional requirements and non-functional system requirements

2. Design description, including architecture, layout, operating modes, and ALARP considerations in the design development

3. Key verification activities identified for substantiation of SSCs

Environment and Security Functional Requirements for SSCs will be reported in the Generic Environment Report (GER) and the Generic Security Report (GSR) respectively and are not included in the scope of the PCSR.

Furthermore, the scope of this chapter covers the mechanical aspects of fluid systems, with the selection of materials and justification of the integrity of SSCs covered in E3S Case Chapter 23: Structural Integrity, Reference [3].

Design/Programme Maturity

RR SMR design information presented in this revision of the E3S Case is largely based on the design definition at the end of Preliminary Concept Definition (PCD), which is an interim design stage representing RD5 level of programme maturity.

PCD is an interim design stage, where SSCs have achieved a level of design maturity, broadly that, requirement specifications are identified and understood, the design scope is defined and bounded, preferred concepts are selected and are likely to deliver requirements, or a plan for down-selection of multiple options is in place, and key verification activities are identified.

6.0.3 Claims, Arguments, Evidence Route Map

The Chapter level Claim for E3S Case Chapter 6: Engineered Safety Features is:

Claim 6: The RR SMR Engineered Safety Features are designed and substantiated to achieve functional and non-functional safety requirements through the lifecycle, and reduce risks to As Low As Reasonably Practicable

A decomposition of this Claim into Sub-Claims, Arguments, and link to the relevant Tier 2 Evidence is provided in Section 6.9, 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].

6.0.4 Applicable Regulations, Codes & Standards

The mechanical systems and components summarised in this report are designed in accordance with their safety classification, to the codes and standards outlined in Table 6.0-1, based on Reference [5].

Table 6.0-1: Mechanical Design Codes & Standards

Safety Classification	Design Basis Code
Very High Reliability (VHR)	American Society of Mechanical Engineers (ASME) III (Sub-section NB) and beyond code requirements
High Reliability (HR)	ASME III (Sub-section NB) and beyond code requirements
Class 1	ASME III
Class 2	ASME III
Class 3	ASME III or Commercial standards e.g., ASME VIII, British Standard BS EN 13445
n/a	Commercial standards e.g., ASME VIII, BS EN 13455

6.1 Emergency Core Cooling Systems & Residual Heat Removal Systems

6.1.1 Emergency Core Cooling System

System and Equipment Functions

The Emergency Core Cooling System (ECCS) [JN01] delivers the Emergency Core Cooling (ECC) Safety Measure to achieve the FSF of Control of Fuel Temperature (CoFT) in response to a range of fault conditions, including most Intact Circuit Faults (ICFs) and Loss of Coolant Accidents (LOCAs).

High-Level Safety Function (HLSFs) for the ECC Safety Measure, and the Postulated Initiating Events (PIEs) against which they are assigned, are being derived in the Fault Schedule, which is presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Safety Design Basis

Functional Requirements

Safety categorised functional requirements are specified for the ECCS [JN01] based on the HLSFs they deliver, including the applicable plant states and operating modes, these are presented in Table 6.1-1.

The traceability of safety categorised functional requirements back to the HLSFs will be managed in DOORS (Dynamic Object-Oriented Requirements System) via the Safety Measures Module; this process is outlined in Deterministic Safety Methodology, Reference [7].

Table 6.1-1: [JN01] Safety Categorised Functional Requirements

DOORS ID	Functional Requirement	Plant State(s)	Mode(s) of Operation	Safety Category
JN01-R-1434	While in Emergency Core Cooling, when at Faulted Operations, the [JN] Reactor Heat Removal Systems shall remove residual heat [JN01]	DBC-3ii DBC-4	1, 2, 3, 4, 5 and 6 when there is fuel in the reactor	A

For each of the safety categorised functional requirements in Table 6.1-1, specific requirements are also derived aligning to each of the PIEs that the ECC Safety Measure is claimed against; these are listed in the DOORS ECCS [JN01] Requirements Module, and not are repeated here, noting all safety categorised functional requirements currently specified for the ECCS [JN01] have a safety category A.

The safety categorised functional requirements for the ECCS [JN01] are flowed down and allocated to relevant sub-systems and/or components in the DOORS ECCS [JN01] Allocated Requirements Module. This functional decomposition is illustrated in the Capella model(s) in DOORS, with the functional interfaces described further in Section 6.1.1.

Non-functional performance requirements associated with the safety categorised functional requirements are also allocated in the DOORS ECCS [JN01] Requirement Module, including the rationale for their selection. These are summarised in Table 6.1-2.

Table 6.1-2: [JN01] Non-Functional Performance Requirements

Associated Functional Requirement	Non-Functional Performance Requirement
JN01-R-1434	The Reactor Heat Removal Systems [JN] shall have a design pressure equal to **{REDACTED}**
	The [JN] Reactor Heat Removal Systems shall have a design temperature equal to **{REDACTED}**
	While in Emergency Core Cooling, when at faulted operations, the Reactor Heat Removal Systems [JN] shall remove residual heat [JN01] with a period without operator intervention greater than or equal to 72 hours
	While in Emergency Core Cooling, when at faulted operations, the Reactor Heat Removal Systems [JN] shall remove residual heat [JN01] with a period without external support greater than or equal to 168 hours
	While in Emergency Core Cooling, when at faulted operations, the Reactor Heat Removal Systems [JN] shall remove residual heat [JN01] with a fuel temperature less than 2785°C
	While in Emergency Core Cooling, when at faulted operations, the Reactor Heat Removal Systems [JN] shall remove residual heat [JN01] with a fuel clad temperature less than 1204°C

Non-Functional System Requirements

Non-Functional System Requirements are specified for the ECCS [JN01] based on the E3S Design Principles. The requirements specified at PCD are listed in the DOORS ECCS [JN01] Requirements Module, including the rationale for their application. These are summarised in Table 6.1-3.

Table 6.1-3: [JN01] Non-Functional System Requirements

DOORS ID	Non-Functional System Requirement	Rationale
JN01-R-1375	While in Emergency Core Cooling, when at Faulted Operation, the [JN01] Reactor Heat Removal Systems shall support a probability of failure on demand lower than 1E-03/demand	Failure probability specified for Class 1 measures in E3S Principles

DOORS ID	Non-Functional System Requirement	Rationale
JN01-R-1527	SMR systems that contain radioactive material shall be designed to prevent spread of that radioactive material beyond their boundary	Confinement of radioactive material for containment and sub-systems in E3S Principles
JN01-R-1528	The Emergency Core Cooling System [JN01] shall have no single points of failure for heat removal	Application of single failure criterion specified for Class 1 measures in E3S Principles

A full set of Non-Functional System Requirements are in development based on the E3S Design Principles, which will be systematically applied to each SSC as part of the systems engineering process. All requirements are subject to refinement and finalisation.

Safety Classification

The ECCS [JN01] is the principal means by which the Category A safety function CoFT is achieved, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2], the highest safety classification of components within the system is Class 1.

Seismic Classification

The seismic classification of SSCs is still to be assigned in accordance with methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2].

Description of SSC

The objective of the ECCS [JN01] is to remove residual heat from the Reactor System [JA] during faulted operation and transfer the heat to the atmosphere. The system architecture can be separated into three phases based on the transient progression following ECCS [JN01] initiation, each described below based on Reference [8].

Phase 1 – Blowdown and Accumulator Injection

On initiation of ECCS [JN01] the Automatic Depressurisation System [JNF] Emergency Blow Down (EBD) valves open, allowing the contents of the Reactor Coolant System (RCS) [JE] to blowdown to the Refuelling Pool [FAF] and the Containment Structure [JMA], rapidly reducing primary circuit pressure.

Three Low Pressure Injection System [JNG] accumulators are provided, each filled with water and pressurised with a nitrogen bubble. In the event the reactor circuit pressure falls below the accumulator pressure, the water from the accumulators will be forced into the Reactor System [JA], re-flooding the Reactor Vessel [JAA}.

Phase 2 – Gravity Drain

When the accumulators have discharged and plant pressure has equalised with containment, the Refuelling Pool [FAF] is aligned to inject coolant to the Reactor System [JA] under gravity. The pools are elevated a minimum height above the Reactor System [JA] to provide sufficient hydrostatic head to drive the coolant in at a flowrate that at least matches the rate at which the coolant is boiled off. The coolant is discharged to the Containment Structure [JMA] as steam via the blowdown line and is collected in the containment sump.

Phase 3 – Recirculation

An injection route is provided to allow coolant collected in the containment sump to be directed back to the Reactor Coolant System [JE]. Hydrostatic head drives coolant into the Reactor System [JA], providing a continued source of decay heat removal. The volume of water available in the Refuelling Pool [FAF] is enough to ensure a sufficient hydrostatic head of water is achieved in the containment sump, to drive flow into the Reactor System [JA] to keep the fuel bundle covered.

Steam generated in the Reactor System [JA] throughout the transient is discharged via a low-pressure blowdown line to the Containment Structure [JMA]. The Local Ultimate Heatsink System (LUHS) [JNK] Passive Containment Cooling (PCC) heat exchangers, located within containment, condense the discharged steam allowing it to collect in the containment sump for recirculation.

The PCC heat exchangers are fed by coolant from the LUHS tank. Heat is transferred from the PCC heat exchangers to coolant within the LUHS tank. As heat is transferred, water in the LUHS tank heats up, boils off and is discharged to atmosphere.

The baseline key performance and design parameters for JN01 are presented in Table 6.1-4.

Table 6.1-4: Key [JN01] System Design and Performance Parameters

Parameter		**Value**
Phase 1 Blowdown and Accumulator Injection	Accumulator Injection Pressure	**{REDACTED}**
	Accumulator Water Volume	**{REDACTED}**
	Accumulator Redundancy	1 out of 3 (1oo3)
Phase 2 Gravity Feed	Gravity Feed Water Volume	**{REDACTED}**
	Peak Injection Rate	**{REDACTED}**
	Injection Line Redundancy	1oo3
Phase 3 Recirculation & Passive Containment Cooling	PCC Heat Exchanger Duty	**{REDACTED}**
	Containment Design Pressure	**{REDACTED}**
	Local Ultimate Heat Sink (LUHS) Water	**{REDACTED}**
	LUHS redundancy	1oo3 to achieve 24 hours 2oo3 to achieve 72 hours

The key sub-systems comprising the Emergency Core Cooling System [JN01] are summarised further below.

Reactor System [JA]

The Reactor System [JA] contains coolant, enabling reflood and subsequent core heat removal. Further details of the Reactor System are presented in E3S Case Chapter 5: Reactor Coolant System and Associated Systems, Reference [9]

Automatic Depressurisation System [JNF]

The Automatic Depressurisation System [JNF] contains both a High Pressure (HP) and Low Pressure (LP) blowdown line to depressurise the Reactor Coolant System [JE] and enable passive coolant injection via the accumulators (phase 1) and gravity drain (phase 2). Each blowdown line contains an EBD valve and Automatic Isolation Valve (AIV) in series to reduce the potential for a spurious Control & Instrumentation (C&I) trip causing inadvertent blowdown.

Low Pressure Injection System [JNG]

The Low-Pressure Injection System (LPIS) [JNG] delivers the accumulator injection, gravity injection from the refuelling pool and the recirculation phase. Detailed information for the LPIS [JNG] is presented in the LPIS System Description, Reference [10].

The system comprises three accumulators sized to provide 1oo3 protection. Each accumulator contains **{REDACTED FOR PUBLICATION}** of water and **{REDACTED FOR PUBLICATION}**. The accumulators are located outside of the Containment Structure [JMA] and are connected to the Reactor System [JA] via Direct Vessel Injection (DVI) nozzles located on the Reactor Vessel [JAA] inlet plenum.

The Refuelling Pool [FAF] is connected to the Reactor System [JA] via the accumulator injection lines. Multiple parallel connections interface with the refuelling pool to control the injection rate and optimise water usage as decay heat falls. Isolation and non-return valves are included in these lines to allow diagnosis and isolation of dormant gravity drain valve failures. Submerged filter screens are located at the entrance to the gravity injection lines to prevent potential debris from entering the Reactor System [JA].

There are three recirculation line connections to the Reactor Pressure Vessel (RPV) downcomers via the accumulator injection lines. The connections include valves for isolation and to prevent backflow into the containment sump. Containment sump screens are located at the entrance of each injection line to prevent ingress of debris into the Reactor System [JA].

Local Ultimate Heatsink System [JNK]

The Local Ultimate Heatsink System [JNK] comprises of three trains, each containing an LUHS tank and its associated ancillary equipment, including the provision of fill, drain and sampling functions. Each LUHS tank corresponds to a single PCC train.

The LUHS tanks are arranged such that each tank (and most of the supporting equipment) is currently located outside containment in the interspace, adjacent to the Steam Generator (SG) with which it interfaces. Cross-connects are provided between each tank to enable the unused water in one tank to be gravity drained into a tank that is available to cool the plant. The final location and geometry of the LUHS tanks are still to be finalised.

The PCC heat exchangers are cooled by water from the LUHS tank, which circulates water in a closed loop between the LUHS tank and PCC heat exchanger via natural circulation.

It is noted that the LUHS [JNK] cooling capability is shared between both the ECCS [JN01] and Passive Decay Heat Sink (PDHR) [JN02] protective safety measures, as well as the mitigative safety measure In-Vessel Retention (IVR) [JM01]. The ECCS [JN01] and IVR [JM01] share the in-containment PCC heat exchangers that are cooled by the LUHS [JNK] water inventory, whereas the heat exchangers located inside the LUHS [JNK] vessels are dedicated to PDHR [JN02] (described in Section 6.1.2).

Containment Structure [JMA]

During an ECC demand, the Containment Structure [JMA] provides a fluid boundary which contains the blowdown of the RCS [JE] and prevents active coolant release to the environment. The containment design pressure is determined by the peak pressure following a design basis LOCA, at the point at which the rate of PCC condensation exceeds the rate of steam generation.

The Containment Structure [JMA] lower head is in-filled with reinforced concrete, such that internal flood-up volume is less than the usable volume of the Refuelling Pool [FAF] for ECC Phase 3 recirculation. The flood-up level necessary to induce the recirculation flowrate requirement is 0.5m, however a conservative flood-up level requirement of 1.0m is placed on the Containment Structure [JMA] to ensure suitable margin.

Further information on the Containment Structure is provided in Section 6.4.

Fuel Pools [FA]

During ECC Phase 2, the Refuelling Pool [FAF] is drained into the Reactor Coolant System [JE] via a series of off takes, located at multiple levels within the pools. These off takes allow the flowrate of coolant to be passively metered throughout gravity drain, reducing the total water volume required during gravity drain. The storage volume of the pool is sized to ensure sufficient coolant (in combination with coolant from the accumulators and Reactor System [JE]) above the flood-up level to induce the recirculation flowrate.

The physical layout of the equipment and subsystems supporting ECCS operation is summarised in Table 2.1-5.

Table 2.1-5: Location of ECCS [JN01] Supporting Equipment

Key Equipment	System Designation	Physical Location Description
Accumulators (x3)	Low Pressure Injection System [JNG]	Accumulators connected direct to Reactor Vessel inlet plenum. Accumulators located outside of containment in the Reactor Auxiliary Building.
Pool and Sump Strainers		All equipment located inside the Containment Structure
Gravity drain and recirculation pipework		
Depressurisation subsystem	Automatic Depressurisation System [JNF]	All equipment located inside the Containment Structure

Table 2.1-5: Location of ECCS [JN01] Supporting Equipment

Key Equipment	System Designation	Physical Location Description
Internal Pool Water Volume	Refuelling Pool [FAF]	Pool located inside the Containment Structure
Passive Containment Cooling Heat Exchanges	LUHS [JNK]	Heat exchangers located on the inside wall of the Containment Structure and connected to the LUHS tanks.
LUHS Tanks (x3) and supporting equipment	LUHS [JNK]	Three independent tanks outside the containment structure and elevated to ensure natural circulation with containment heat exchangers.
Containment Isolation Valves	Various primary systems	Valves located as close as possible to the containment boundary.

SSC Operation

The Reactor Island Operating Philosophy, Reference [11], provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode. This is summarised in E3S Case Chapter 13: Conduct of Operations, Reference [12].

SSC Configuration

During Operating Modes 1 (Power Operation), 2 (Low Power) and 3 (Hot Standby), the following key Emergency Core Cooling System [JN01] components are aligned in the following configuration:

1. [JEG] HP Blowdown Automatic Isolation Valves – Closed
2. [JEG] HP EBD Valves – Closed
3. [JEG] LP Blowdown Automatic Isolation Valves – Closed
4. [JEG] LP EBD Valves – Closed
5. [JNG] Accumulator Isolation Valves – Open
6. [JNG] Gravity Drain Isolation Valves – Closed
7. [JNG] Recirculation Isolation Valves – Closed
8. [JNK] Passive Containment Cooling Isolation Valves – Open

During Operating Modes 4a (Hot Shutdown – Steaming), 4b (Hot Shutdown – Non-Steaming) and 5a (Cold Shutdown – Pressurised), although plant pressure and temperature are reduced below their operating conditions, the use of cold leg saturation conditions as a means of initiation allows the ECCS [JN01] to continue in standby, as per Mode 1, without a change to trip configuration.

LPIS [JNG] accumulators are isolated on primary circuit pressure reaching 8.0MPa to prevent accumulator injection during planned plant pressure reduction. Conversely, during start-up, accumulator isolation valves are opened on plant pressure reaching 8.0MPa. The accumulator isolation valves are opened automatically in event of ECCS [JN01] initiation while primary circuit pressure is below 8.0MPa.

EBD valve protection against spurious ECCS [JN01] initiation is removed on plant pressure reducing below 7.5MPa; however, the EBD valve main body actuator will remain in the shut position, unless a blowdown path is created via the downstream AIV opening. EBD valve start-up and shutdown procedures will be developed in future design stages.

During Operating Mode 6a (Refuelling with Reduced Water Level above Fuel) it is expected that the ECCS [JN01] will be available via manual initiation.

During Operating Mode 6B (Refuelling with Water Level above Fuel at Nominal Full) the LUHS tanks, accumulators and PCC heat exchangers will be able to be sequentially drained down for Examination, Maintenance, Inspection and Testing (EMIT). Each of these components are arranged with redundancy allowing two trains always to be kept online as they could be required to support the ECCS [JN01]. The EMIT schedule for ECCS [JN01] is still to be developed.

SSC Operation during Power Operation (Mode 1)

No operator action is required to control temperature during the first 72 hours of Emergency Core Cooling [JN01] operation, however, the operator can confirm successful alignment and sustained heat transfer through monitoring of Reactor Vessel [JAA] level and temperature.

As the inventory control boundary is extended from the RCS[JE] to the Containment Structure [JMA], it is necessary to isolate the containment vessel and connected systems on initiation of the ECCS [JN01]. This isolation function is yet to be fully defined, though it will include isolation of all containment fluid penetrations, excluding the accumulators and PCC connection to the LUHS.

No operator action is required to control inventory during ECCS [JN01] operation. However, the operator can confirm] inventory is maintained through monitoring of Refuelling Pool [FAF] and Containment Structure [JMA] sump level.

No operator action is required for pressure control during the first 72 hours of ECCS [JN01] operation. Beyond 72 hours, the operator will observe the fall in LUHS level from the Main Control Room (MCR) and once both LUHS are at a low-level limit (to be determined), the operator will remotely align the third (casualty) LUHS tank to drain by gravity into a non-casualty LUHS tank. Long-term cooling solutions (once all three LUHS tanks are empty) are still to be defined.

Specific responses to faults include:

1. Small LOCAs: In the event of continued inventory loss, the pressuriser will empty resulting in the eventual loss of plant overpressure and generation of saturation conditions in the RCS[JE] cold leg, which will initiate ECC[JN01]. In the event of a sustained loss of heat

removal, plant temperatures will gradually increase until saturation conditions are reached and ECCS [JN01] is initiated

2. Intermediate LOCAs: To ensure that the pressure is reduced rapidly to enable gravity drain prior to exceeding fuel temperature limits, HP EBD is used to reduce plant pressure from saturation pressure down to a low pressure (<7MPa), which ensures the accumulators can inject and maintain RPV level. Following accumulator injection, the LP EBD further reduces pressure to equalise with containment pressure and enable gravity feed injection

3. Large LOCAs: Immediate loss of pressure control and rapid blow down of the RCS [JE] to the Containment Structure [JMA] results in saturation conditions in the RCS [JE] and initiation of ECCS [JN01]

4. LOCA in DVI line: Similar to a large or intermediate LOCA, however the rate at which the Refuelling Pool [FAF] drains would increase, prompting early transition from gravity drain to recirculation

5. Unisolable Steam Generator Tube Rupture (SGTR): During primary to secondary leaks such as SGTR, containment isolation is not claimed as part of ECCS [JN01] to provide functional diversity from PDHR. Instead, the LUHS tanks can be drained into the Containment Structure [JMA] sump to maintain total system inventory. Coolant then circulates from the sump to the Reactor Vessel [JAA] via the LPIS [JNG] recirculation pipework providing decay heat removal. This is known as ‘ECC boil-off’

6. Other Intact Primary Circuit faults: Should Condenser Decay Heat Removal (DHR) (at DiD level 2) or PDHR fail to provide continued heat removal, an increase in Reactor Coolant System [JE] coolant temperature will lead to eventual saturation conditions in the RCS [JE], thus resulting in initiation of the ECCS [JN01]

Materials

The description and justification of materials used for Class 1 SSCs are presented in E3S Case Chapter 23: Structural Integrity, Reference [3].

Interfaces with Supporting Systems

The key ECCS[JN01] interfaces are identified and managed within DOORS, including flow down of functional requirements, and presented below in Table 6.1-6.

Table 6.1-6: [JN01] Interfaces

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-5540	FA – Spent Fuel System	The Spent Fuel Systems [FA] shall supply water for emergency core cooling to the Emergency Core Cooling System [JN01]
SMR-IF-11361	JE – Reactor Coolant System	The Reactor Coolant System [JE] shall supply reactor coolant to the Emergency Core Cooling System [JN01] for high pressure blowdown

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-11362	JE – Reactor Coolant System	The Reactor Coolant System [JE] shall supply reactor coolant to the Emergency Core Cooling System [JN01] for low pressure blowdown
SMR-IF-6462	JA – Reactor System	The Emergency Core Cooling System [JN01] shall supply coolant to the Reactor System [JA] to support temperature and inventory control
SMR-IF-11256	JA – Reactor System	The Reactor System [JA] shall transfer heat from fuel to coolant
SMR-IF-7026	JM – Reactor Plant Containment Systems	The Reactor Plant Containment Systems [JM] shall supply coolant to the Emergency Core Cooling System [JN01] recirculation
SMR-IF-6470	KN – Liquid Waste Treatment Systems	The Liquid Waste Treatment Systems [KN] shall supply treated coolant to the Emergency Core Cooling System [JN01] for accumulator fill
SMR-IF-6475	QJ – Central Gas Supply System	The Central Gas Supply System [QJ] shall supply high pressure nitrogen to the Emergency Core Cooling System [JN01] for accumulator gas pressurisation
SMR-IF-6472	KL – Heating, ventilation, air conditioning (HVAC) system	The Emergency Core Cooling System [JN01] shall supply accumulator discharge gas to the HVAC system [KL]
SMR-IF-12327	KU – Sampling Systems	The Emergency Core Cooling System [JN01] shall supply coolant to the Sampling Systems [KU] for accumulator sampling

Instrumentation & Control

The Reactor C&I System [JY] is required to initiate ECCS [JN01] and low-pressure blowdown. The Reactor C&I System [JY] will also monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the emergency control centre. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. The envisaged requirements for trips, monitoring, indication, alarms, and warnings are specified in the ECCS System Description, Reference [8].

The allocation of safety categorised functional requirements from the ECCS [JN01] to the Reactor C&I System [JY] is presented in the C&I Engineering Schedule, described further in E3S Case Chapter 7: Instrumentation & Control, Reference [13].

Monitoring, Inspection, Testing & Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of the ECCS [JN01] will need to be replaced within that period. An outline maintenance plan for the ECCS [JN01] is still to be developed.

Radiological Aspects

During operation of the ECCS [JN01], the Containment Structure [JMA] provides the safety function to maintain coolant inventory, preventing release of radioactive coolant to the environment.

A subset of fault sequences, known as 'ECC Boil-Off', includes initiating events such as SGTR for which containment isolation is not claimed, resulting in a loss of coolant from containment and the potential for increased exposures. Doses associated with these fault sequences are estimated to be low and broadly acceptable, whilst the boil-off provision ensures functional diversity between ECCS [JN01] and PDHR [JN02].

Performance and Safety Evaluation

Compliance with Safety Categorised Functional Requirements

At PCD, verification strategies for the ECCS [JN01] to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements are in development and stored in DOORS, including:

1. RELAP Plant Performance and GOTHIC Containment Analysis

2. Thermal-hydraulic rig testing to validate model analysis

The full suite of performance analysis to justify that the ECCS [JN01] achieves its safety categorised functional requirements and associated non-functional performance requirements for bounding fault conditions will be presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Prior to PCD, performance analysis has been conducted to support the concept design development and its optimisation; this is presented in the ECCS [JN01] System Description, Reference [8]. As the analysis is based on a pre-PCD baseline design and does not provide verification of the current design requirements, it has not been repeated here.

Compliance with Non-Functional System Requirements

The methods to demonstrate compliance against non-functional system requirements assigned to the ECCS [JN01] are presented in the DOORS ECCS [JN01] Verification Module. The status of compliance at PCD is:

1. Probability of failure on demand target of 1E-03 (JN01-R-1375): early sensitivity studies for previous ECCS [JN01] design configurations against Core Damage Frequency (CDF) have provided confidence that reliability targets can be met. Further Probabilistic Safety Assessment (PSA) for the most recent ECCS [JN01] design configuration is required to demonstrate compliance

2. Design to prevent spread of radioactive material beyond their boundary (JN01-R-1527): to be confirmed through inspection

3. Design has no single points of failure (JN01-R-1528): the accumulators, gravity drain, and recirculation pipework are arranged in a 1oo3 configuration respectively, to ensure the

ECCS [JN01] can achieve its safety function in the event a train is lost to both the initiating event and random single failure

Installation & Commissioning

An outline installation and commissioning plan for the ECCS [JN01] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [14].

ALARP in Design Development

The design of the ECCS [JN01] has been developed in accordance with the systems engineering design process, which includes alignment to Relevant Good Practice (RGP) and Operating Experience (OPEX), design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant E3S criteria (as described in E3S Case Chapter 1: Introduction, Reference [1]).

Key ECCS [JN01] design decisions made with respect to ensuring overall risks are reduced to ALARP include:

1. Optioneering of redundancy arrangements has resulted in the selection of DVI and 1oo3 redundancy for the accumulator architecture, and 1oo3 redundancy for the phase 2 gravity drain lines. This decision is based on RGP for improved single failure tolerance over 2oo3 designs, and minimising reliance on structural integrity arguments for RCS pipework.

2. Various containment cooling options have been considered, including cooling by heat exchangers with dedicated water supply and containment surface spray. A containment surface spray system is considered to add significant complexity with respect to tank structural supports, due to the additional elevation of water mass and containment surface features for water distribution. A PCC heat exchanger located within containment and cooled by the LUHS has been selected as the preferred option, based on reduced complexity and RGP, with other options placing safety categorised ventilation requirements on the containment interspace.

3. The LUHS [JNK] cooling capability is shared between both the ECCS [JN01] and PDHR [JN02] protective safety measures, as well as the mitigative safety measure IVR [JM01]. Further heatsink diversity and risk reduction are incorporated into the design of the RR SMR through the provision of an Atmospheric Steam Dump. An evaluation of heatsink diversity has demonstrated that the design solution is consistent with UK and international RGP, including International Atomic Energy Agency (IAEA), European Utility Requirements (EUR) and other Pressurised Water Reactor (PWR) designs, and is capable of achieving suitable levels of DiD and achieving numerical targets

More detailed information on design decisions is presented in the ECCS System Description, Reference [8], and associated design decision files.

Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 6.0.2. Key design opportunities and decisions related to nuclear safety currently being explored include:

1. LUHS tank size, configuration, and location are to be optimised, with further consideration of the decay heat profile to provide the necessary decay heat removal; the long-term cooling requirements (up to 168 hours); and tolerance to internal hazards

2. LPIS water volume is to be confirmed following accumulator optimisation for Large LOCA faults and containment layout development resulting in an increased Refuelling Pool [FAF] volume

3. Category A functional requirements on the Steam Generator Relief Valves to provide decay heat removal during the initial stages of an Intermediate LOCA

All design development risks and opportunities are captured and managed by design teams.

6.1.2 Passive Decay Heat Removal

System and Equipment Functions

The Passive Decay Heat Removal (PDHR) [JN02] system delivers the PDHR Safety Measure to achieve the FSF of CoFT in response to a range of fault conditions, including most ICFs and small LOCAs.

HLSFs for the PDHR Safety Measure, and the PIEs against which they are assigned, are being derived in the Fault Schedule, which is presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Safety Design Basis

Functional Requirements

Safety categorised functional requirements are specified for the PDHR [JN02] based on the HLSFs they deliver, including the applicable plant states and operating modes, these are presented in Table 6.1-7.

The traceability of safety categorised functional requirements back to the HLSFs will be managed in DOORS via the Safety Measures Module; this process is outlined in Deterministic Safety Methodology, Reference [7].

Table 6.1-7: [JN02] Safety Categorised Functional Requirements

DOORS ID	Functional Requirement	Plant State(s)	Mode(s) of Operation	Safety Category
JN02-R-1527	While in faulted operations, the Passive Decay Heat Removal [JN02] shall remove residual heat	DBC-2 DBC-3 DBC-4	1, 2, 3, 4, 5a	B

For each of the safety categorised functional requirements in Table 6.1-7, specific requirements are also derived aligning to each of the PIEs that the PDHR Safety Measure is claimed against; these are listed in the DOORS PDHR [JN02] Requirements Module, and are not repeated here, noting all safety categorised functional requirements currently specified for the PDHR [JN02] have a safety category B.

The safety categorised functional requirements for the PDHR [JN02] are flowed down and allocated to relevant sub-systems and/or components in the DOORS PDHR [JN02] Allocated Requirements Module. This functional decomposition is illustrated through the DOORS Capella model(s), with the functional interfaces described further in Section 6.1.2.

Non-functional performance requirements associated with the safety categorised functional requirements are also allocated in the DOORS PDHR [JN02] Requirements Module, including the rationale for their selection. These are summarised in Table 6.1-8.

Table 6.1-8: [JN02] Non-Functional Peformance Requirements

Associated Functional Requirement	Non-Functional Performance Requirement
JN02-R-1527	The Reactor Heat Removal Systems [JN] shall have a design pressure (for SSC which form part of the primary pressure boundary) equal to **{REDACTED}**
	The [JN] Reactor Heat Removal Systems shall have a design temperature (for SSC which form part of the primary pressure boundary) equal to **{REDACTED}**
	The Reactor Heat Removal Systems [JN] shall have a design pressure (for SSC which form part of the secondary pressure boundary) equal to **{REDACTED}**
	The [JN] Reactor Heat Removal Systems shall have a design temperature (for SSC which form part of the secondary pressure boundary) equal to **{REDACTED}**
	While in faulted operations, the Passive Decay Heat Removal [JN02] shall remove residual heat with a period without operator intervention greater than or equal to 72 hours
	While in faulted operations, the Passive Decay Heat Removal [JN02] shall remove residual heat with a period without external support following initiation greater than or equal to 168 hours
	While in faulted operations, following a DBC-2ii fault, the Passive Decay Heat Removal [JN02] shall ensure Departure from Nucleate Boiling does not occur on any fuel rod surface with 95% probability, with 95% confidence
	While in faulted operations, following a DBC-3 fault, the Passive Decay Heat Removal [JN02] shall prevent 95% of fuel rods from experiencing Departure from Nucleate Boiling
	While in faulted operations, following a DBC-4 fault, the Passive Decay Heat Removal [JN02] shall prevent 90% of fuel rods from experiencing Departure from Nucleate Boiling
	While in faulted operations, Passive Decay Heat Removal [JN02] shall remove residual heat [JN02] with a fuel temperature less than 2785°C

Associated Functional Requirement	**Non-Functional Performance Requirement**
	While in faulted operations, following a DBC-4 fault, the Passive Decay Heat Removal [JN02] shall remove residual heat [JN02] with a fuel clad temperature less than 1204°C

Non-Functional System Requirements

Non-functional system requirements are specified for the PDHR [JN02] based on the E3S Design Principles. The requirements specified at PCD are listed in the DOORS PDHR [JN02] Requirements Module, including the rationale for their application. These are summarised in Table 6.1-3.

Table 6.1-3: [JN02] Non-Functional System Requirements based on E3S Design Principles

DOORS ID	**Non-Functional System Requirement**	**Rationale**
JN02-R-1569	SMR systems that contain radioactive material shall be designed to prevent spread of that radioactive material beyond their boundary	Confinement of radioactive material for containment and sub-systems in E3S Principles
JN02-R-1570	The Passive Decay Heat Removal [JN02] system shall have no single points of failure for heat removal	Loss of cooling to the spent fuel pool could result in fuel cladding breach

A full set of non-functional system requirements are in development based on the E3S Design Principles, which will be systematically applied to each SSC as part of the systems engineering process. All requirements are subject to refinement and finalisation.

Safety Classification

The PDHR [JN02] is the secondary means by which the Category A safety function CoFT is achieved, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2], the highest safety classification of components within the system is Class 2.

Seismic Classification

The seismic classification of SSCs is still to be assigned in accordance with methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2].

Description of SSC

The objective of the PDHR [JN02] is to remove decay heat from the reactor core during faulted operation and transfer the heat to the atmosphere. This system is described below based on Reference [15].

The baseline architecture for the PDHR safety measure consists of three cooling trains, each aligned to an RCS [JE] loop. The three cooling trains are independent and configured such that 2oo3 trains can provide 72 hours of decay heat removal (noting changes to this baseline configuration are planned following PCD, described in paragraph 0).

Decay heat is transferred from the fuel assemblies [JAK] to RCS [JE] coolant. This coolant flows through the loops to the Steam Generation System [JEA] where the secondary water boils to generate pressurised steam. Steam is transferred from the SG to the Main Steam System [LBA], and onwards to a dedicated PDHR heat exchanger in the Passive Steam Condensing System (PSCS) [JNB].

The steam is then condensed through heat transfer into a body of water located in the LUHS [JNK]; the condensed coolant falls by gravity through PSCS [JNB] drain lines to the Feedwater System [LA], and water in the LUHS [JNK] boils to atmosphere to provide ultimate heat removal from the power station. This process is passive and does not rely on pumped flow from the Reactor Coolant Pumps (RCPs).

Inventory of the primary coolant needs to be maintained during operation of the PDHR [JN02] due to contracting coolant as the temperature falls, and due to losses of coolant during a small LOCA fault. Inventory control can be provided by any one of the following three systems, initiated upon detection of low level in the pressuriser:

1. Level and Volume Control System (LVCS) [KBA] (details of this system are provided in E3S Case Chapter 5: Reactor Coolant System & Associated Systems, Reference [9])

2. High Pressure Injection System (HPIS) [JND] should the LVCS [KBA] be unavailable

3. Low Pressure Injection System (LPIS) [JNG] should the LVCS [KBA] and HPIS [JND] be unavailable

Secondary inventory is controlled through isolation of connecting systems to the SG upon detection of low level in the SG.

Primary circuit pressure control is maintained through operation of the pressuriser heaters to sustain the Pressuriser steam bubble in the Reactor Coolant Pressurising System [JEG]. If the heaters are unavailable, then the HPIS [JND] will be initiated to increase pressure. The LPIS [JNG] may also be used for a small sub-set of faults where the pressuriser empties.

Secondary circuit pressure control may require passive lift of the SG safety relief valves or actuation of the power operated steam relief valves to provide overpressure protection in the event of some fault sequences (e.g., Complete Loss of Heat Sink). The PDHR [JN02] architecture is illustrated in Figure 6.1-1, and key design and performance parameters are summarised in Table 6.1-4.

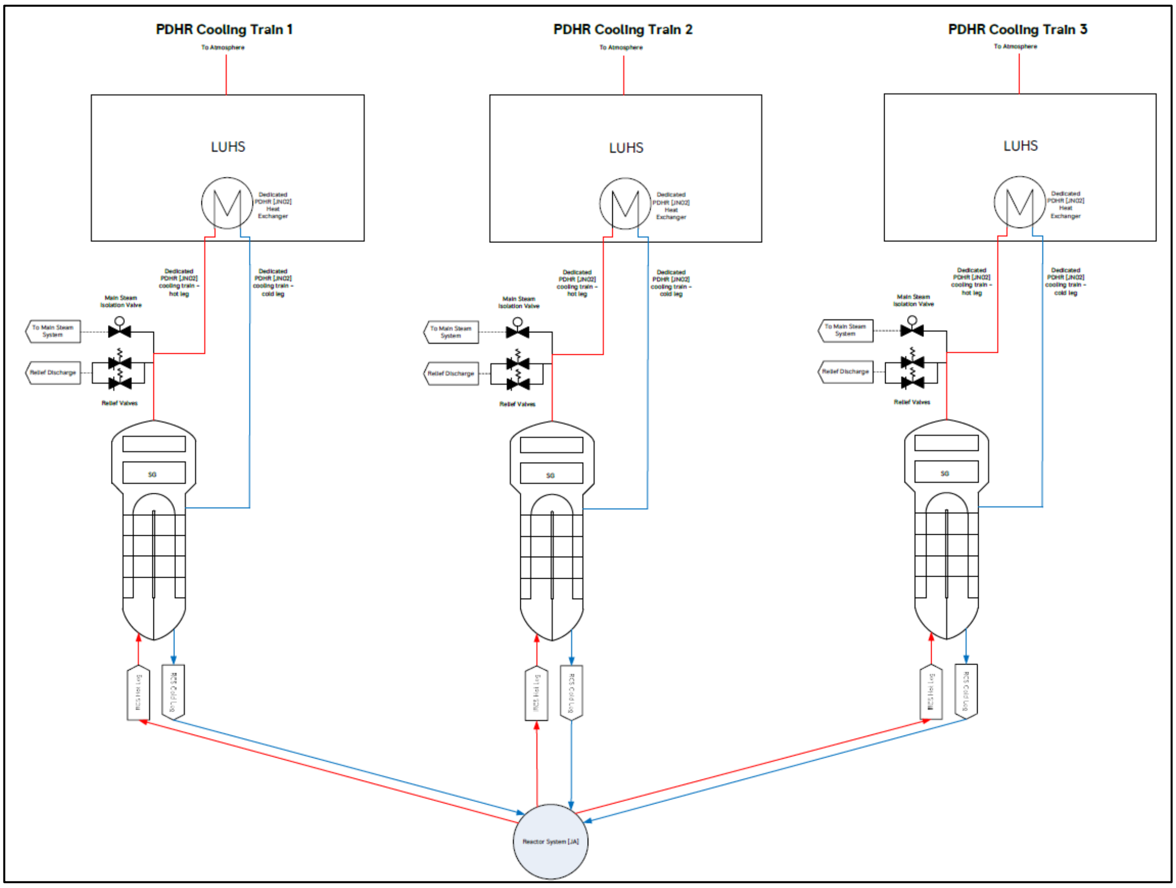


Figure 6.1-1: PDHR [JN02] Cooling Train Architecture

Table 6.1-4: Key Design & Performance Parameters for PDHR [JN02]

Parameter	**Value**
Maximum Fuel Clad Temperature	1204°C
PDHR [JN01] Maximum Duty	**{REDACTED FOR PUBLICATION}**
Maximum RCS [JE] Operating Pressure	**{REDACTED FOR PUBLICATION}**
Minimum RCS [JE] Operating Pressure	**{REDACTED FOR PUBLICATION}**
Minimum RCS [JE] Temperature (cold leg)	**{REDACTED FOR PUBLICATION}**
Maximum RCS [JE] Temperature (hot leg)	**{REDACTED FOR PUBLICATION}**
Maximum SGS [JE] Operating Pressure (Secondary)	**{REDACTED FOR PUBLICATION}**
Maximum LUHS [JNK] Operating Temperature	**{REDACTED FOR PUBLICATION}**
Maximum LUHS [JNK] Operating Pressure	**{REDACTED FOR PUBLICATION}**

All the sub-systems comprising the PDHR [JN02] are outlined in the PDHR System Description, Reference [15]. Details of the dedicated sub-systems are summarised further below.

Passive Steam Condensing System [JNB]

The PSCS [JNB] sub-system is dedicated to supporting the PDHR safety measure. It is a closed loop steam condensing system, which receives heated steam from the SGs via a penetration on the Main Steam System [LBA], located in the portion of the main steam piping upstream of the main steam isolation valve and inside the containment building.

Pipework transfers steam to the PSCS [JNB] heat exchanger, which is located within the LUHS [JNK] tank. The heat exchanger transfers heat to the water in the tank, condensing the steam in the tubes. The condensate is subsequently returned to the main feed line via a penetration, which is in the main feed line piping downstream of the main feed isolation valve and inside the containment building.

The hot and cold legs of pipework each contain two valves, situated either side of the containment boundary. These valves are normally open (except for one normally shut valve on the hot leg), which as well as supporting containment isolation, is also used for initiation and isolation of the PDHR safety measure. To ensure PDHR [JN02] can passively initiate upon a Station Blackout (SBO), the single normally shut isolation valve is required to reliably fail open upon loss of power.

Further details of the PSCS [JNB] are provided in the System Description, Reference [16].

Local Ultimate Heat Sink [JNK]

The LUHS [JNK] arrangement is described in Section 6.1.1.

High Pressure Injection System [JND]

The primary function of the HPIS [JNB] is to supply coolant to the RCS [JE] at high pressure during PDHR [JN02] safety function operation, compensating for water volume contraction in the RCS [JE] during ICFs and water loss through the leak site during a small LOCA.

The baseline architecture for the HPIS [JNB] consists of two independent trains of injection and recirculation. Each train includes an injection line from the LOCA water storage pools to the RPV DVI connections and a recirculation line from the containment sump to the LOCA water storage pools to recover coolant lost due to the leak, with a 1oo2 configuration.

Each train has one High Pressure (HP) pump (termed a HPIS injection pump) used for injection into the RPV at Normal Operating Pressure (NOP), and one sump recirculation pump (termed a HPIS recirculation pump), which is used to transfer coolant collected in the containment sump back to the LOCA water storage pools for re-injection.

It is noted the HPIS [JND] also provides high pressure makeup capability to the ASF [JD02], injecting soluble boron to shut down the reactor in event of Scram [JD01] failure (described in Section 6.2.2).

Further details of the HPIS [JNB] are provided in the HPIS System Description, Reference [17].

Low Pressure Injection System [JNG]

The LPIS [JNG] arrangement is described in Section 6.1.1.

SSC Operation

The Reactor Island Operating Philosophy, Reference [11], provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode. This is summarised in E3S Case Chapter 13: Conduct of Operations, Reference [12].

SSC Configuration

During Operating Mode 1 (Power Operation), the following key PDHR [JN02] components are aligned in the following configuration:

1. PDHR Initiation Valves – Closed
2. Main Steam Isolation Valves (MSIVs) – Open
3. HPIS Injection Line Isolation Valves – Closed
4. HPIS Recirculation Valves – Closed
5. HPIS Injection Pump – Off
6. HPIS Recirculation Pump – Off

During Operating Mode 2 (Start-Up), the trips will be reset to their powered operation values, at which point PDHR [JN02] will be available and configured as per Mode 1.

During Operating Modes 3 (Hot Standby), 4a (Hot Shutdown – Steaming), 4b (Hot Shutdown – Non-Steaming), 5a (Cold Shutdown – Pressurised), and 5b (Cold Shutdown – Depressurised), the PDHR will be available in standby and configured as per Mode 1.

During Operating Mode 6a (Refuelling with Reduced Water Level above Fuel) the heat removal function will be deactivated in preparation for maintenance during Operating Mode 6B (Refuelling with Reduced Water Level above Fuel at Nominal Full).

Faulted Operation

PDHR [JN02] is automatically initiated upon detection of low level in two of the three SGs, including the following actions:

1. Shut the MSIVs, Atmospheric Steam Dump isolation valves and SG Blowdown [LCQ] valves connected to each SG
2. Open the PDHR hot leg isolation valve

These steps can also be manually initiated from the MCR.

If available, the CVCS [KB] will continue to provide automatic level control following the fault to maintain Pressuriser water level in its normal operating bands and the Pressuriser heaters / spray will maintain pressure control.

If the CVCS [KB] pumps fail or a small LOCA occurs, HPIS [JND] is automatically initiated upon receipt of a pressuriser low level signal, including the following actions:

1. Open the Injection Line Containment Isolation Valves
2. Open the Injection Line Control Valves
3. Open the Recirculation Line Containment Isolation Valves
4. Open the Recirculation Line Control Valves
5. Turn on Injection Pump
6. Turn on Recirculation Pump (2 on duty)

All connecting systems to the RCS [JE] are also isolated.

The operating philosophy for the HPIS [JNB] during PDHR operating modes Is still to be confirmed. In the event both CVCS [KB] and HPIS [JNB] are unavailable, LPIS [JND] is initiated automatically when the pressure falls below 7.0MPa. The long-term- design solution for the LUHS inventory control following a prolonged period (>72 hours) of PDHR [JN01] is still to be developed.

Specific operating responses to a range of fault conditions are presented in the PDHR System Description, Reference [15].

Materials

The description and justification of materials used for Class 2 SSCs are presented in E3S Case Chapter 23: Structural Integrity, Reference [3].

Interfaces with Supporting Systems

The key PDHR [JN02] interfaces are identified and managed within DOORS, including flow down of functional requirements, and summarised below in Table 6.1-5.

Table 6.1-5: PDHR [JN02] Interfaces

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-11244	Reactor System [JA]	Transfers heat from the fuel to the RCS [JE] coolant
SMR-IF-11239	Reactor Coolant System [JE]	Transfers coolant from the Reactor System [JA] to the Steam Generator.
SMR-IF-11267	Steam Generating System [JEA]	Transfers coolant to the Main Steam System [LBA], generates steam, senses SG level and isolates SG blowdown.
SMR-IF-11282	Reactor Coolant Pressurising System [JEF]	Senses pressuriser level and pressure
SMR-IF-11275	Reactor Coolant Pressure Relief System [JEG]	Isolates leaks in the relief system and senses pressure relief line flow

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-11285	Cold Shutdown Cooling System [JNA]	Isolates leaks in the Cold Shutdown Cooling System [JNA] from the RCS [JE]
SMR-IF-2198	Reactor Plant C&I Systems [JY]	Supplies control signals and supply electrical data signals
SMR-IF-11261	Chemistry and Volume Control System [KB]	Isolates leaks in the Chemistry and Volume Control System [KB] from the Reactor Coolant System [JE]
SMR-IF-11288	Reactor Sampling System [KUA]	Isolates leaks in the Reactor Sampling System [KUA] from the Reactor Coolant System [JE]
SMR-IF-6478	Main Feed System [LA]	Transfers coolant from the PSCS [JNB] to the SGs
SMR-IF-7027	Main Steam System [LB]	Transfer steam from the SGs to the PSCS [JNB], isolates steam flow to the turbines, initiates and isolates atmospheric steam dump flow, relieves steam and senses SG pressure

Instrumentation & Control

PDHR [JN02] places several trip functions onto the Reactor C&I System [JY] for initiation. The Reactor C&I System [JY] will also monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the emergency control centre. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. The envisaged requirements for trips, monitoring, indication, alarms, and warnings are specified in the PDHR System Description, Reference [15].

The allocation of safety categorised functional requirements from the PDHR [JN02] to the Reactor C&I System [JY] is presented in the C&I Engineering Schedule, described further in E3S Case Chapter 7: Instrumentation & Control, Reference [13].

Monitoring, Inspection, Testing & Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of the PDHR [JN02] will need to be replaced within that period. An outline maintenance plan for the PDHR [JN02] is still to be developed.

Radiological Aspects

No significant radiological aspects associated with the PDHR [JN02] operation have been identified during design decisions up to PCD.

Performance and Safety Evaluation

Compliance with Safety Categorised Functional Requirements

At PCD, verification strategies for the PDHR [JN02] and associated sub-systems to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements are in development and stored in DOORS, including:

1. RELAP Plant Performance Analysis

2. Integrated Effects Testing to validate RELAP Plant Performance Analysis

3. PSCS Heat Exchanger and LUHS Tank Thermal Stratification Test to validate RELAP Plant Performance Analysis for hydraulic recirculation between the heat exchanger and the tank

Prior to PCD, analysis has been conducted to support the concept design development and its optimisation; this is presented in the PDHR [JN02] System Description, Reference [15]. The analysis is based on early RELAP methods and does not provide verification of the current design requirements; therefore, it has not been repeated here.

The full suite of analysis to justify that the PDHR [JN01] achieves its safety categorised functional requirements and associated non-functional performance requirements for bounding fault conditions will be presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Compliance with Non-Functional System Requirements

Verification activities to substantiate non-functional system requirements for PDHR [JN02] are still to be determined.

Installation & Commissioning

An outline installation and commissioning plan for the PDHR [JN02] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [14].

ALARP in Design Development

The design of the PDHR [JN02] has been developed in accordance with the systems engineering design process, which includes alignment to RGP & OPEX, design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant safety criteria (as described in E3S Case Chapter 1: Introduction, Reference [1]).

More detailed information on design decisions is presented in the PDHR System Description, Reference [15], and associated design decision files.

Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 6.0.2. Key design opportunities and decisions related to nuclear safety are currently being explored, this includes:

1. Safety requirements are to be placed on either the Power Operated SG Relief Valves or Passive SG Relief Valves for secondary pressure control, dependent on further assessment of fault conditions with consideration of appropriate diversity with the ECCS [JN01]

2. A decision to increase redundancy of the PDHR cooling train and heat exchanger architecture from 2oo3 to 1oo3 to improve the reliability of the system, is expected to be reflected in the Final Concept Definition (FCD) design baseline

3. Hazard protection requirements to ensure the PDHR [JN02] is tolerant to internal and external hazards are to be established, dependent on further hazards analysis

All design development risks and opportunities are captured and managed by design teams.

6.2 Emergency Reactivity Control Systems

6.2.1 Scram [JD01]

System and Equipment Functions

The Scram Function [JD01] delivers the Scram Safety Measure to achieve the FSF of Control of Reactivity (CoR) in response to a range of fault conditions, including most ICFs and LOCAs.

HLSF for the Scram Safety Measure, and the PIEs against which they are assigned, are being derived in the Fault Schedule, which is presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Safety Design Basis

Functional Requirements

Safety categorised functional requirements are specified for the Scram [JD01] based on the HLSFs they deliver, including the applicable plant states and operating modes, these are presented in Table 6.2-6.

The traceability of safety categorised functional requirements back to the HLSFs will be managed in DOORS via the Safety Measures Module; this process is outlined in Deterministic Safety Methodology, Reference [7].

Table 6.2-6: [JD01] Safety Categorised Functional Requirements

DOORS ID	Functional Requirement	Plant State(s)	Mode(s) of Operation	Safety Category
JD01-R-1271	During faulted operations, when Scram is demanded, the SCRAM Safety Function [JD01] shall shutdown the reactor	DBC-2ii DBC-3i DBC3ii DBC-4	1, 2	A

For each of the safety categorised functional requirements in Table 6.2-6, specific requirements are also derived aligning to each of the PIEs that the Scram Safety Measure is claimed against (including internal and external hazards); these are listed in the DOORS Scram Function [JD01] Requirements Module, and not are repeated here, noting all safety categorised functional requirements currently specified for the Scram Function [JD01] have a safety category A.

The safety categorised functional requirements for the Scram Function [JD01] are flowed down and allocated to relevant sub-systems and/or components in the DOORS Scram Function [JD01] Allocated Requirements Module. This functional decomposition is illustrated through the DOORS Capella model(s), with the functional interfaces described in Section 6.1.1.

Non-functional performance requirements associated with the safety categorised functional requirements are also allocated in the DOORS Scram Function [JD01] Requirements Module, including the rationale for their selection. These are summarised in Table 6.2-2.

Table 6.2-2: [JD01] Non-Functional Performance Requirements

Associated Functional Requirement	**Non-Functional Performance Requirement**
JD01-R-1271	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a reactivity (Keff) less than 0.99 (shutdown acceptance criteria with a single failure)
	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a target probability of failure on demand less than 1E-04/demand
	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a reactivity (Keff) less than 0.95 (shutdown acceptance criteria)
	The Scram Function [JD01] shall have a design temperature (for SSC which form part of the primary pressure boundary) equal to **{REDACTED}**
	The Scram Function [JD01] shall have a design pressure (for SSC which form part of the primary pressure boundary) equal to **{REDACTED}**
	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a fuel linear heat rate for un-poisoned pins limit less than 73.8kW/m
	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a fuel linear heat rate for poisoned pins limit less than 55.4kW/m
	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a margin to nucleate boiling ratio limit less than 1.3
	During Faulted Operations, when Scram is demanded, the Scram Function [JD01] shall shutdown the reactor with a reactivity (Keff) limit less than 1 + β

Non-Functional System Requirements

Non-functional system requirements are specified for the Scram Function [JD01] based on the E3S Design Principles. The requirements specified at PCD are listed in the DOORS Scram Function [JD01] Requirements Module, including the rationale for their application. These are summarised in Table 6.2-3.

Table 6.2-3: [JD01] Non-Functional System Requirements based on E3S Design Principles

DOORS ID	Non-Functional System Requirement	Rationale
JD01-R-1444	Systems that contain radioactive material shall be designed to prevent spread of that radioactive material beyond their boundary	Confinement of radioactive material for containment and sub-systems in E3S Principles
JD02-R-1445	The Scram Function [JD01] system shall have no single points of failure for reactivity control during faulted modes	Scram is subject to the single failure criterion

A full set of non-functional system requirements are in development based on the E3S Design Principles, which will be systematically applied to each SSC as part of the systems engineering process. All requirements are subject to refinement and finalisation.

Safety Classification

The Scram Function [JD01] is the principal means by which the Category A safety function CoR is achieved, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2], the highest safety classification of components within the system is Class 1.

Seismic Classification

The seismic classification of SSCs is still to be assigned in accordance with methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2].

Description of SSC

The objective of the Scram Function [JD01] is to provide reactivity control during faulted operation by inserting negative reactivity in the form of solid neutron absorbers into the reactor fuel, thereby shutting down the reactor.

A soluble boron-free chemistry regime for duty reactivity control and the Scram Function [JD01] has been developed for the RR SMR, meaning that full shutdown margin can be achieved by the control rods without the addition of boron.

Scram relies on successful insertion of the Control Rods [JDE] with associated Control Rod Drive Mechanisms (CRDMs) [JDA]. It is also reliant on instrumentation predominantly within the Reactor Coolant System [JE] and response of the Reactor Control and Protection Systems [JY]. The baseline configuration of the Scram Function [JD01] is presented in the schematic in Figure 6.2-1, and key design and performance parameters are summarised in Table 6.2-4.

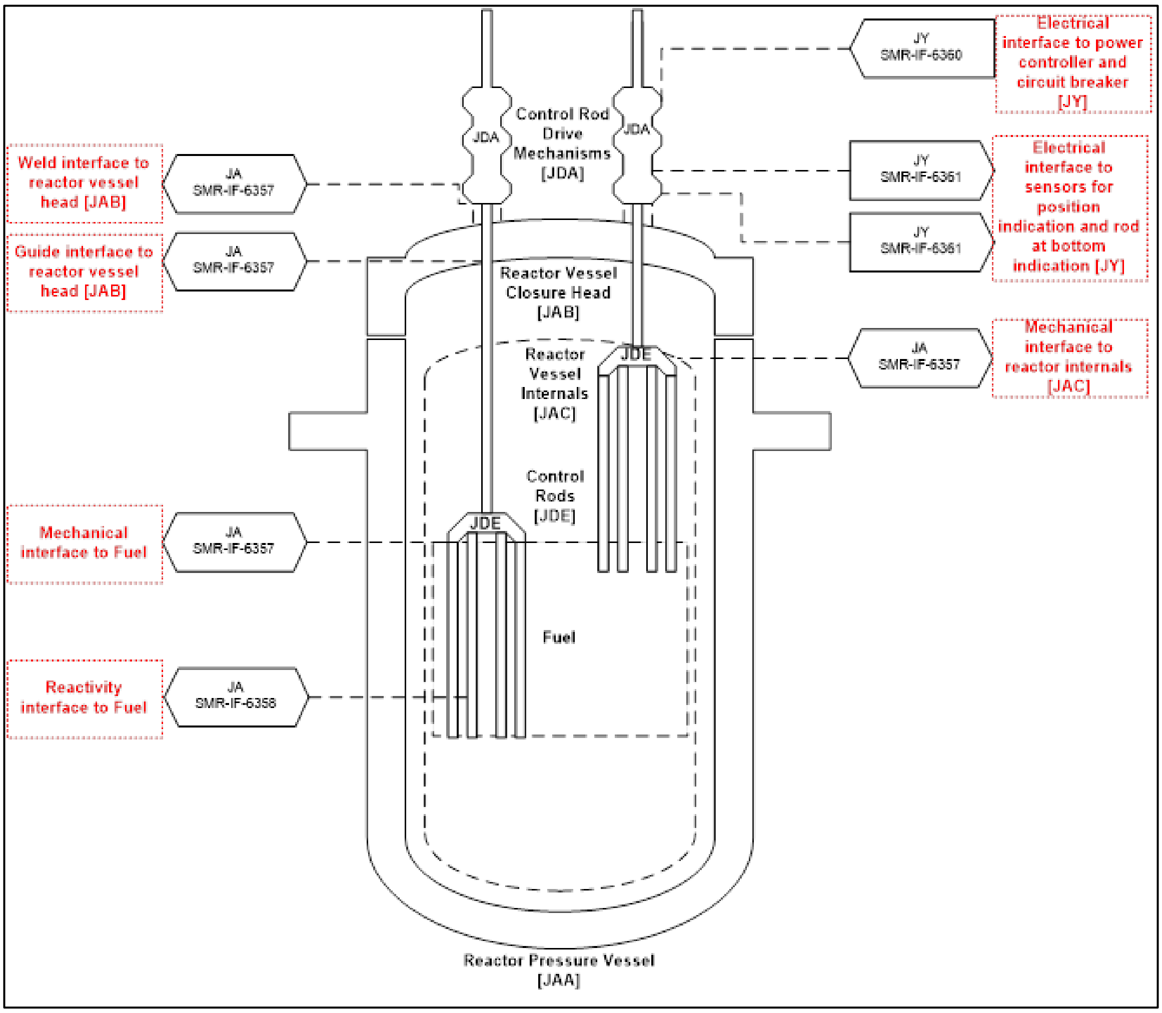


Figure 6.2-1: Duty Reactivity Control and Scram [JD01] Schematic

Table 6.2-4: Key Design & Performance Parameters for Scram Function [JD01]

Parameter	**Value**
Target Minimum Departure from Nuclear Boiling Ratio (DNBR)	>1.3
Target Maximum Linear Heat Rate	<73.8kW/m for un-poisoned fuel pins <55.4kW/m for poisoned (up to 8w/o Gd) fuel pins
Maximum Time to Initiate	3.4s
Maximum Allowable Power	105% Full Power
Number of Rods Required for Shutdown	108 (N-1)
Target Reliability (Probability of Failure on Demand)	~ 1E-04

The baseline architecture for the Scram Function [JD01] is outlined in the Scram System Description, Reference [18]. Details of the dedicated sub-systems are summarised further below.

Control Rod Drive Mechanisms [JDA]

The CRDMs [JDA] control the physical position of the Control Rods [JDE], for both powered operations, including start-up and planned shutdown operations, and support insertion of the Control Rods into the reactor in the event of a fault where rapid shutdown is required. The CRDMs [JDA] also provide a fluid boundary for reactor coolant within the Reactor System [JA]. The current design includes 113 CRDMs.

Control Rods [JDE]

The Control Rods [JDE] provide solid neutron absorption to control reactivity within the Reactor System [JA] during powered operation, start-up and planned shutdown operations, and rapid shutdown of the reactor in the event of fault. The current design includes 113 control rods with associated CRDMs [JDA].

Reactor Control & Protection System [JY]

The Reactor Control & Protection System [JY] provides the initiation function for Scram Function [JD01] based on reaching set points and parameters to ensure prompt response to the full range of fault conditions for which it is claimed.

The Scram Function [JD01] is delivered by two independent and diverse control systems within the Reactor Control & Protection System [JY], the Safety Class 2 Reactor Protection System [JR] and the Safety Class 1 Diverse Protection System [JQ], each capable of isolating power to the CRDMs [JDA].

A redundant voting logic system will be used (at PCD this is 2oo3), with 3 sensors for each measured parameter, and power supply aligned such that loss of power will also cause the system to automatically trip.

SSC Operation

The Reactor Island Operating Philosophy, Reference [11], provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode. This is summarised in E3S Case Chapter 13: Conduct of Operations, Reference [12].

SSC Configuration

During Operating Mode 1 (Power Operation), the Scram Function [JD01] will be on standby, monitoring plant parameters to trip when traversing outside of the operational set points. The CRDMs [JDA] will be in use and will either be holding the Control Rods [JDE] at the required position in the core to achieve the desired power and temperature for the reactor plant or moving rod position to achieve the desired power and temperature.

During Operating Mode 2 (Start-Up) as the rods are gradually withdrawn to provide reactivity addition, the Scram Function [JD01] will be monitoring predominantly reactor flux conditions in order to trip should reactivity start increasing at a rate which is outside permissible limits.

During Operating Mode 3 (Hot Standby), the Scram Function [JD01] is not required as the Control Rods [JDE] will be fully inserted, providing reactivity hold down.

During Operating Mode 4a (Hot Shutdown – Steaming), 4b (Hot Shutdown – Non-Steaming), 5a (Cold Shutdown – Pressurised), and 5b (Cold Shutdown – Depressurised), rod withdrawal is not required, therefore it is expected that electrical power to the drive mechanisms will be disconnected to avoid inadvertent reactivity addition.

During Operating Mode 6a (Refuelling with Reduced Water Level above Fuel) and 6B (Refuelling with Reduced Water Level above Fuel at Nominal Full), the Control Rod Drive Mechanisms [JDA] will be removed to access in the Reactor Pressure Vessel [JAA] internals. The Scram Function [JD01] is unavailable during this procedure, and electrical power to the drive mechanisms will remain isolated to avoid an electrical fault contributing to the risk of rod withdrawal.

Faulted Operation

The primary function of the Scram Function [JD01] is to provide a principal role in the CoR during plant faulted operations. Following a monitored parameter reaching a trip condition (or loss of electrical power supply), the Reactor Protection System [JR] and the Diverse Protection System [JQ] will provide commands to interrupt the power supplies to the CRDMs [JDA] that are holding the Control Rods [JDE] at a defined position in the core, causing them to drop and become fully inserted in the core by use of gravity. This provides sufficient reactivity suppression to prevent criticality (with some margin) down **{REDACTED FOR PUBLICATION}.**

The design of the control rods is such that even with one rod of the highest worth stuck in position fully withdrawn from the core, the remaining rods are still capable of maintaining reactivity hold down, though with a reduced margin.

At least two parameters are identified for each fault sequence to provide protection. The trip parameters and response for each fault sequence are listed in the Scram System Description, Reference [18].

Materials

The description and justification of materials used for Class 1 SSCs are presented in E3S Case Chapter 23: Structural Integrity, Reference [3].

Interfaces with Supporting Systems

The key Scram Function [JD01] interfaces are identified and managed within DOORS, including flow down of functional requirements, and summarised below in Table 6.2-5.

Table 6.2-5: Scram Function [JD01] Interfaces

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-6538	Reactor System [JA]	The Reactor Reactivity Control Systems [JD] shall provide reactivity control for the Reactor System [JA]

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-6360	Reactor Control System [JY]	The Reactor Control System [JY] shall control power supply to the Reactor Reactivity Control Systems [JD]
SMR-IF-6362		The Reactor Control System [JY] shall initiate the safety functions of the Reactor Reactivity Control Systems [JD]
SMR-IF-6361		Reactor Reactivity Control Systems [JD] shall supply measurement data to the Reactor Control System [JY]

Instrumentation & Control

The Scram Function [JD01] places several trip functions onto the Reactor C&I System [JY] for initiation. The Reactor Control System [JY] will also monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the emergency control centre, enabling the manual initiation of the Scram Function [JD01].

It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. The envisaged requirements for trips, monitoring, indication, alarms, and warnings are specified in the Scram System Description, Reference [18].

The allocation of safety categorised functional requirements from the Scram Function [JD01] to the Reactor C&I System [JY] is presented in the C&I Engineering Schedule, described further in E3S Case Chapter 7: Instrumentation & Control, Reference [13].

There is no requirement for electrical power for the Scram Function [JD01] to actuate, and loss of electrical power will cause the Scram Function [JD01] to initiate.

Monitoring, Inspection, Testing & Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of the Scram Function [JD01] will need to be replaced within that period. An outline maintenance plan for the PDHR [JN02] is still to be developed.

Radiological Aspects

No significant radiological aspects associated with the Scram Function [JD01] operation have been identified during design decisions up to PCD. It is noted the decision for RR SMR to deliver boron-free duty reactivity control can contribute to a reduction in exposures during normal operation due to reduced tritium generation.

Performance and Safety Evaluation

Compliance with Safety Categorised Functional Requirements

At PCD, verification strategies for the Scram Function [JD01] and associated sub-systems to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements are in development and stored in DOORS, including:

1. RELAP Plant Performance Analysis

2. Core flow and boron mixing rig testing to validate analysis

3. A CRDM verification strategy proposed by chosen vendor

Prior to PCD, analysis has been conducted to support the concept design development and its optimisation; this is presented in the Scram Function [JD01] System Description, Reference [18]. The analysis is based on early RELAP methods and does not provide verification of the current design requirements; therefore, it has not been repeated here.

The full suite of analysis to justify that the Scram Function [JD01] achieves its safety categorised functional requirements and associated non-functional performance requirements for bounding fault conditions will be presented in E3S Case Chapter 15: Safety Analysis, Reference [6] as performance analysis evidence is developed.

Compliance with Non-Functional System Requirements

Verification activities to substantiate non-functional system requirements for Scram Function [JD01] are still to be determined.

Installation & Commissioning

An outline installation and commissioning plan for the Scram Function [JD01] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [14].

ALARP in Design Development

The design of the Scram Function [JD01] has been developed in accordance with the systems engineering design process, which includes alignment to RGP and OPEX, design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant safety criteria (as described in E3S Case Chapter 1: Introduction, Reference [1]).

Key Scram Function [JD01] design decisions made with respect to ensuring overall risks are reduced to ALARP include:

1. Control rods (without boron injection) have been selected as the method of reactivity control given the RR SMR plant decision to be boron-free, providing advantages over a boron option including increased passivity and simplification of the Class 1 system, significant reduction in tritium generation, elimination of boron dilution faults, and reduced corrosion and radiation fields due to a high constant pH chemistry regime

More detailed information on design decisions is presented in the Scram System Description, Reference [18], and associated design decision files.

Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 6.0.2. Key design opportunities and decisions related to nuclear safety are currently being explored, this includes:

1. Continued development of the core design will consider the implementation of a rod ejection prevention feature within the CRDM [JDA] to prevent uncontrolled reactivity addition due to control rod ejection, in combination with supplier engagement. The number of control rods will continue to evolve as the core design matures

All design development risks and opportunities are captured and managed by design teams.

6.2.2 Alternative Shutdown Function [JD02]

System and Equipment Functions

The Alternative Shutdown Function (ASF) [JD02] provides the secondary means to achieve the FSF of CoR in response to a range of fault conditions, including most ICFs and small LOCAs.

HLSFs for the ASF [JD02], and the PIEs against which they are assigned, are being derived in the Fault Schedule, which is presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Safety Design Basis

Functional Requirements

Safety categorised functional requirements are specified for the ASF [JD02] based on the HLSFs they deliver, including the applicable plant states and operating modes, these are presented in Table 6.2-6.

The traceability of safety categorised functional requirements back to the HLSFs will be managed in DOORS via the Safety Measures Module; this process is outlined in Deterministic Safety Methodology, Reference [7].

Table 6.2-6: [JD02] Safety Categorised Functional Requirements

DOORS ID	Functional Requirement	Plant State(s)	Mode(s) of Operation	Safety Category
JD02-R-1273	While in Alternative shutdown function, the Alternative Shutdown Function [JD02] shall shutdown the reactor	DBC-4	1, 2	B

For each of the safety categorised functional requirements in Table 6.2-6, specific requirements are also derived aligning to each of the PIEs that the ASF [JD02] is claimed against (including internal and external hazards); these are listed in the DOORS ASF [JD02] Requirements Module, and not are repeated here, noting all safety categorised functional requirements currently specified for the ASF [JD02] have a safety category B.

The safety categorised functional requirements for the ASF [JD02] are flowed down and allocated to relevant sub-systems and/or components in the DOORS ASF [JD02] Allocated Requirements Module. This functional decomposition is illustrated through the DOORS Capella model(s), with the functional interfaces described in Section 6.2.2.

Non-functional performance requirements associated with the safety categorised functional requirements are also allocated in the DOORS ASF [JD02] Requirements Module, including the rationale for their selection. These are summarised in Table 6.2-7.

Table 6.2-7: [JD02] Non-Functional Performance Requirements

Associated Functional Requirement	Non-Functional Performance Requirement
JD02-R-1273	During Faulted Operations, when Alternative Shutdown Function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a margin to nucleate boiling ratio limit less than 1.3
	During Faulted Operations, when Alternative shutdown function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a fuel linear heat rate for un-poisioned pins limit less than 73.8kW/m
	During Faulted Operations, when Alternative shutdown function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a reactivity (Keff) limit less than 1 + β
	During Faulted Operations, when Alternative shutdown function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a reactivity (Keff) less than 0.95 (shutdown acceptance criteria)
	During Faulted Operations, when Alternative shutdown function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a fuel linear heat rate for poisioned pins limit less than 55.4kW/m
	During Faulted Operations, when Alternative shutdown function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a reactivity (Keff) with a single failure less than 0.99 (shutdown acceptance criteria)
	During Faulted Operations, when Alternative shutdown function is demanded, the Alternative Shutdown Safety Function [JD02] shall shutdown the reactor with a target probability of failure on demand less than 1E-04/demand
	The Alternative Shutdown Safety Function [JD02] shall have a design temperature (for SSC which form part of the primary pressure boundary) equal to **{REDACTED}**
	The Alternative Shutdown Safety Function [JD02] shall have a design pressure (for SSC which form part of the primary pressure boundary) equal to **{REDACTED}**.

Non-Functional System Requirements

Non-functional system requirements are specified for the ASF [JD02] based on the E3S Design Principles. The requirements specified at PCD are listed in the DOORS ASF [JD02]

Requirements Module, including the rationale for their application. These are summarised in Table 6.2-8.

Table 6.2-8: [JD02] Non-Functional System Requirements based on E3S Design Principles

DOORS ID	Non-Functional System Requirement	Rationale
JD02-R-1579	Systems that contain radioactive material shall be designed to prevent spread of that radioactive material beyond their boundary	Confinement of radioactive material for containment and sub-systems in E3S Principles
JD02-R-1581	The Alternative Shutdown Function [JD02] system shall have no single points of failure for reactivity control during faulted modes	Loss of reactivity control in a fault could result in core damage

A full set of non-functional system requirements are in development based on the E3S Design Principles, which will be systematically applied to each SSC as part of the systems engineering process. All requirements are subject to refinement and finalisation.

Safety Classification

The ASF [JD02] is the secondary means by which the Category A safety function CoR is achieved, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2], the highest safety classification of components within the system is Class 2.

Seismic Classification

The seismic classification of SSCs is still to be assigned in accordance with methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2].

Description of SSC

The objective of the ASF [JD02] is to provide the secondary means of CoR during faulted operation by inserting negative reactivity in the form of liquid neutron absorbers (boron) into the reactor fuel, thereby shutting down the reactor.

The baseline architecture for the ASF [JD02] is comprised of the Emergency Boron Injection System [JDK]; with a boron storage tank, two supply lines and two metering pumps; and the HPIS [JND] high-head pumps to deliver boron into the Reactor System [JA]. The ASF [JD02] also utilises instrumentation predominantly within the RCS [JE] and response of the Reactor Control and Protection Systems [JY].

The function operation is split into two phases:

1. Phase 1: Concentrated boron solution injection into the Reactor System [JA] directly from the boron storage tank

2. Phase 2: Metered boron injection for any subsequent plant make-up

The key design and performance parameters are summarised in Table 6.2-9.

Table 6.2-9: Key Design & Performance Parameters for ASF [JD02]

Parameter	**Value**
Target Fuel Clad Temperature	< 1204°C
Maximum Fuel Centreline Temperature	< 2785°C
Required Boron Concentration for Cold Zero Power	**{REDACTED FOR PUBLICATION}**
Response Time	~ 30 seconds
Target Reliability (Probability of Failure on Demand)	~ 2E-03

The baseline configuration of the ASF [JD02] is presented in the schematic in Figure 6.2-2.

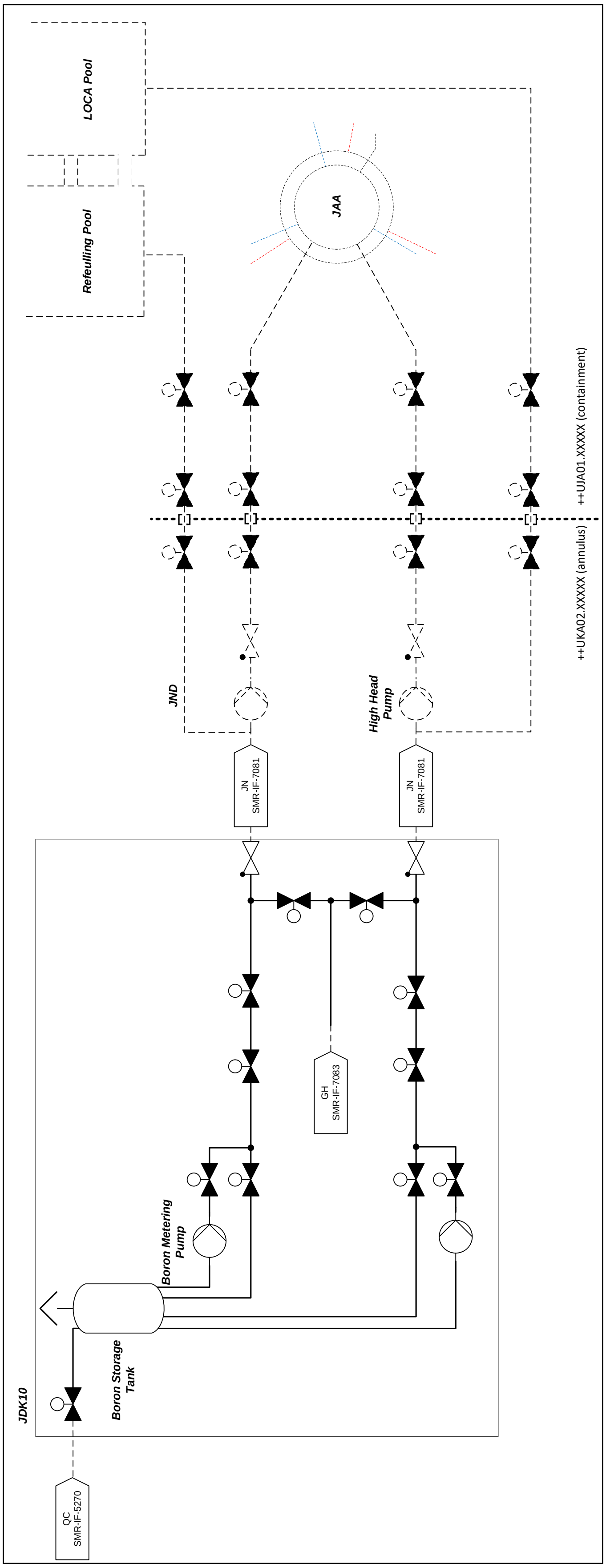


Figure 6.2-2: ASF [JD02] Schematic

The baseline architecture for the ASF [JD02] is outlined in the Alternative Shutdown Function System Description, Reference [19]. Details of the dedicated sub-systems are summarised further below.

Emergency Boron Injection System [JDK]

The Emergency Boron Injection System [JDK] delivers concentrated potassium tetraborate solution to the HPIS [JND], which ultimately directs boron into the Reactor System [JA]. Comprised of two independent trains; each containing a metering pump, valves, pipework, and instrumentation, and drawing from a single boron storage tank, which holds concentrated and enriched boron solution. The system operates at low pressure and is dependent on the HPIS [JND] pumps.

Further details of the Emergency Boron Injection System [JDK] are provided in the Emergency Boron Injection System Description, Reference [20].

High Pressure Injection System [JDK]

The HPIS [JDK] provides the driving head needed to overcome the Reactor System [JA] operating pressure and deliver boron for shutdown. When the ASF [JD02] is tripped, the HPIS [JND] valves on two independent trains are aligned to draw directly from the boron storage tank (and not from the LOCA pools), injecting approximately 5 tonnes of concentrated boron solution into the Reactor System [JA].

Any further demands on the HPIS [JND] pumps, due to low level detected in the pressuriser will cause the Emergency Boron Injection System [JDK] metering pumps to deliver a 1:40 ratio of boron solution to make-up water, to maintain the desired boron concentration within the Reactor System [JA] and RCS [JE].

It is noted the HPIS [JND] also provides high pressure coolant to the RCS [JE] during PDHR [JN02] operation (described in Section 6.1.2).

Further details of the HPIS [JNB] are provided in the HPIS System Description, Reference [17].

Reactor Control & Protection System [JY]

The Reactor Control & Protection System [JY] provides the initiation function for ASF [JD02] based on reaching set points and parameters to ensure prompt response to the full range of fault conditions for which it is claimed.

Independent initiation parameters and sensors are used between the Scram Function [JD01] and the Alternative Shutdown Function [JD02] to achieve required diversity. In any fault requiring Scram, the Scram Function [JD01] would be initiated by two diverse control systems, the Reactor Protection System [JR] and the Diverse Protection System [JQ]. The Alternative Shutdown Function [JD02] is initiated by the Reactor Protection System [JR], so reactivity control remains available in the event of a failure of either the Reactor Protection System [JR] or the Diverse Protection System [JQ].

To avoid the possibility of a spurious or unintended/unrequired injection of boron, the initiation parameters and set points have been selected to ensure that the Scram Function [JD01] will have had the opportunity to have successfully actuated first. A redundant voting logic system will also be used (currently assumed to be 2oo3).

SSC Operation

The Reactor Island Operating Philosophy, Reference [11], provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode. This is summarised in E3S Case Chapter 13: Conduct of Operations, Reference [12].

SSC Configuration

During Operating Mode 1 (Power Operation), the ASF [JD01] will be on standby, monitoring plant parameters to trip when traversing outside of the operational set points, and if the Scram Function [JD01] has failed.

During Operating Mode 2 (Start-Up) as the rods are gradually withdrawn to provide reactivity addition, the ASF [JD02] will also be tripped if the flux parameters measured by the Scram Function [JD01] continue to exceed limits.

During Operating Mode 3 (Hot Standby), the ASF [JD02] is not required as the Control Rods [JDE] will be fully inserted, providing reactivity hold down. The ASF [JD02] will remain available to enable criticality to be achieved when required.

During Operating Mode 4a (Hot Shutdown – Steaming), 4b (Hot Shutdown – Non-Steaming), 5a (Cold Shutdown – Pressurised), and 5b (Cold Shutdown – Depressurised), rod withdrawal is not required, therefore it is expected that the ASF [JD02] will remain in standby.

During Operating Mode 6a (Refuelling with Reduced Water Level above Fuel) and 6B (Refuelling with Reduced Water Level above Fuel at Nominal Full), the Control Rod Drive Mechanisms [JDA] will be removed to access in the Reactor Pressure Vessel [JAA] internals. The feasibility and benefit of placing requirements on the ASF [JD02] to provide reactivity control for refuelling faults is still to be determined.

Faulted Operation

The primary function of the ASF [JD02] is to provide a diverse role in the CoR during plant faulted operations. The operating principles for the Alternative Shutdown Function [JD02] are split into two phases:

1. Phase 1: Following a monitored parameter reaching a trip condition including confirmation that the rods have not already been inserted, the Reactor Protection System [JR] will provide a command to the High-Pressure Injection System [JND] pumps to start, drawing boron directly from the Emergency Boron Injection System [JDK] and injecting into the Reactor Pressure Vessel [JAA} downcomer

2. Phase 2: Once the boron storage tank level drops below the amount required for safe shutdown, the direct suction lines in the Emergency Boron Injection System [JDK] will be isolated. The metering pumps within the Emergency Boron Injection System [JDK] will supply sufficient boron to maintain the required ratio for shutdown [1:40] to the HPIS [JND] pump, should there be any further make-up demands

In either phase, the boron flow rates will be sufficient to provide sufficient reactivity suppression to prevent criticality (with some margin) down **{REDACTED FOR PUBLICATION}.**

The design of the injection volume for Phase 1 is to account for the volume of a fully water solid plant at cold temperatures.

A minimum of one parameter is identified for each fault sequence to provide protection. Parameters selected are also above (or below) that which would have caused the Scram Function [JD01] to trip. The trip parameters and response for each fault sequence are listed in the ASF System Description, Reference [19].

The Reactor Protection System [JR] also isolates the Chemical and Volume Control System (CVCS) [KB] during ASF [JD02] initiation to prevent boron dilution by the CVCS Charging Pumps or Ion Exchange Resins.

Materials

The description and justification of materials used for Class 2 SSCs are presented in E3S Case Chapter 23: Structural Integrity, Reference [3].

Interfaces with Supporting Systems

The key ASF [JD02] interfaces are identified and managed within DOORS, including flow down of functional requirements, and summarised below in Table 6.2-10.

Table 6.2-10: ASF [JD02] Interfaces

Interface ID	Interfacing SSC	Function Interface Summary
SMR-IF-7081	Reactor Heat Removal Systems [JN]	The Reactor Reactivity Control Systems [JD] shall supply borated coolant to the Reactor Heat Removal Systems [JN]
SMR-IF-6462	Reactor System [JA] Reactor Heat Removal Systems [JN]	The Reactor Heat Removal Systems [JN] shall supply coolant to the Reactor System [JA]
SMR-IF-5721	Central Chemicals Supply [QC]	The Central Chemicals Supply [QC] shall supply boronated coolant to the Reactor Reactivity Control Systems [JD]
SMR-IF-7083	Water Treatment Distribution System [GH]	The Distribution systems after water treatment [GH] shall supply demineralised water to the Reactor Reactivity Control Systems [JD]
SMR-IF-6360	Reactor Control System [JY]	The Reactor Control System [JY] shall control power supply to the Reactor Reactivity Control Systems [JD]
SMR-IF-6362		The Reactor Control System [JY] shall initiate the safety functions of the Reactor Reactivity Control Systems [JD]
SMR-IF-6361		Reactor Reactivity Control Systems [JD] shall supply measurement data to the Reactor Control System [JY]

Instrumentation & Control

The ASF [JD02] places several trip functions onto the Reactor C&I System [JY] for initiation. The Reactor Control System [JY] will also monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the emergency control centre, enabling the manual initiation of the ASF [JD02].

It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. The envisaged requirements for trips, monitoring, indication, alarms, and warnings are specified in the ASF System Description, Reference [19].

The allocation of safety categorised functional requirements from the ASF [JD02] to the Reactor C&I System [JY] is presented in the C&I Engineering Schedule, described further in E3S Case Chapter 7: Instrumentation & Control, Reference [13].

ASF [JD02] requirements placed on the emergency power supplies following Loss of Offsite Power (LOOP) faults are still to be determined.

Monitoring, Inspection, Testing & Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of the ASF [JD02] will need to be replaced within that period. An outline maintenance plan for the ASF [JD02] is still to be developed.

Due to the RR SMR duty reactivity being boron-free, maintenance and testing of the ASF [JD02] will be limited to functional tests of distributed parts of sub-systems.

Radiological Aspects

No significant radiological aspects associated with the ASF [JD02] operation have been identified during design decisions up to PCD. It is noted the selection of HPIS [JND] to deliver boron minimises additional plant equipment from a dedicated system, hence reducing the EMIT burden and associated potential for exposures.

Performance and Safety Evaluation

Compliance with Safety Categorised Functional Requirements

At PCD, verification strategies for the ASF [JD02] and associated sub-systems to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements are in development and stored in DOORS, including:

1. RELAP Plant Performance Analysis

2. Core flow and boron mixing rig testing to validate analysis

Prior to PCD, analysis has been conducted to support the concept design development and its optimisation; this is presented in the ASF System Description, Reference [19]. The analysis is based on early RELAP methods and does not provide verification of the current design requirements; therefore, it has not been repeated here.

The full suite of analysis to justify that the ASF [JD02] achieves its safety categorised functional requirements and associated non-functional performance requirements for bounding fault conditions will be presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Compliance with Non-Functional System Requirements

Verification activities to substantiate non-functional system requirements for ASF [JD02] are still to be determined.

Installation & Commissioning

An outline installation and commissioning plan for the ASF [JD02] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [14].

ALARP in Design Development

The design of the ASF [JD02] has been developed in accordance with the systems engineering design process, which includes alignment to RGP & OPEX, design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant safety criteria (as described in E3S Case Chapter 1: Introduction, Reference [1]).

Key ASF [JD02] design decisions made with respect to ensuring overall risks are reduced to ALARP include:

1. The use of HPIS [JND] to inject boron into the RCS [JE] was selected over options such as the RCPs [JEB] or high-pressure gas, providing relative safety benefits including minimisation of boron dilution faults and reduced complexity in the design to enable EMIT

2. The use of a boron storage tank was selected over options such as borated accumulators or a powdered boron tank, providing relative safety benefits including reduced complexity of the ECCS [JN01] and reduced potential for boron crystallisation or undissolved boron powder leading to failure of valves or pumps

More detailed information on design decisions is presented in the ASF System Description, Reference [19], and associated design decision files.

Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 6.0.2. Key design opportunities and decisions related to nuclear safety are currently being explored, this includes:

1. Further design and performance analysis is required to ascertain that the HPIS [JND] can meet both the requirements of ASF [JD02] and PDHR [JN02]. As such, the option for ASF [JD02] to utilise a dedicated high-head pump for boron injection remains open

All design development risks and opportunities are captured and managed by design teams.

6.3 Safety Features for Stabilisation of the Molten Core

6.3.1 In-Vessel Retention

The IVR [JM01] Safety Measure delivers the FSF of CoFT during a core melt, DEC-B accident condition. The main systems contributing to delivery of the IVR [JM01], include:

1. Reactor Vessel Cavity Injection System (RVCIS) [JNM], which transfers coolant from the Refuelling Pool [FAF] to flood the RPV cavity. As coolant passes the RPV [JAA], decay heat is transferred from the corium to the water with steam released into containment

2. PCC heat exchangers, which condense the steam released into containment to provide the primary means of heat removal (additional means of diverse heat removal are being explored as the design matures)

3. RPV [JAA], which provides the retention function of the core melt

4. RPV Insulation [JAH], which provides a flow path around the RPV to promote heat removal

5. Depressurisation system

A simplified schematic is illustrated in Figure 6.3-1.

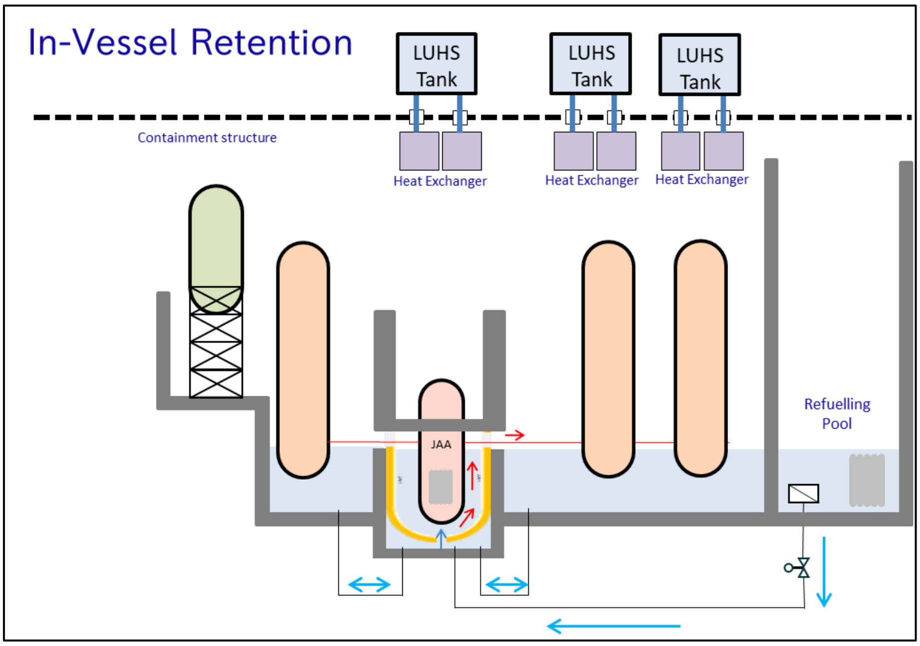


Figure 6.3-1: IVR [JM01] Schematic

At PCD, the IVR [JM01] Safety Measure is in the early stages of development, as such, further details will be presented in future revisions of the E3S Case as the design and associated evidence matures.

6.4 Containment & Associated Systems

6.4.1 Containment Functional Requirements

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.2 Primary Containment System

System and Equipment Functions

The Containment Vessel Structure [JMA] delivers the FSF of Confinement of Radioactive Material (CoRM) during normal and fault conditions.

HLSFs for the Containment Vessel Structure [JMA], and the PIEs against which they are assigned, are being derived in the Fault Schedule, which is presented in E3S Case Chapter 15: Safety Analysis, Reference [6].

Safety Design Basis

Functional Requirements

Safety categorised functional requirements are specified for the Containment Vessel [JMA] based on the HLSFs they deliver, including the applicable plant states and operating modes, these are presented in Table 6.4-1.

The traceability of safety categorised functional requirements back to the HLSFs will be managed in DOORS via the Safety Measures Module; this process is outlined in Deterministic Safety Methodology, Reference [7].

Table 6.4-1: [JMA] Safety Categorised Functional Requirements

DOORS ID	Functional Requirement	Plant State(s)	Mode(s) of Operation	Safety Category
JMA-R-1492	The Containment Vessel Structure [JMA] shall perform its' confinement function when subjected to Design Basis plant conditions.	DBC-1 DBC-2i DBC-2ii DBC-3i DBC-3ii DBC-4	1, 2, 3, 4, 5, 6a, 6b	A
JMA-R-1323	The Containment Vessel Structure [JMA] shall confine radioactive substances within the Containment Boundary during Normal Operation.	DBC-1 DBC-2i	1, 2, 3, 4, 5	C
JMA-R-1324	The Containment Vessel Structure [JMA] shall confine radioactive substances within the	DBC-2ii DBC-3i	1, 2, 3, 4, 5	A

DOORS ID	Functional Requirement	Plant State(s)	Mode(s) of Operation	Safety Category
	Containment Boundary during a Design Basis Accident.	DBC-3ii DBC-4		
JMA-R-1325	The Containment Vessel Structure [JMA] shall confine radioactive substances within the Containment Boundary during a DEC.	DEC-A DEC-B	1, 2, 3, 4, 5	C
JMA-R-1328	The Containment Vessel Structure [JMA] shall meet the SMR Release Rate Targets.	DBC-1 DBC-2i DBC-2ii DBC-3i DBC-3ii DBC-4	1, 2, 3, 4, 5, 6a, 6b	A
JMA-R-1330	The Containment Vessel Structure [JMA] shall protect systems within Containment from Internal Hazards originating outside of the Containment boundary.	TBC	1, 2, 3, 4, 5, 6a, 6b	A
JMA-R-1524	The Containment Vessel Structure [JMA] shall protect systems outside Containment from Internal Hazards originating inside of the Containment boundary.	TBC	1, 2, 3, 4, 5, 6a, 6b	A
JMA-R-1524	The Containment Vessel Structure [JMA] shall retain its structural integrity in the event of a Design Basis External Hazard.	TBC	1, 2, 3, 4, 5, 6a, 6b	A
JMA-R-1515	The Containment Vessel Structure [JMA] shall be designed to limit, in all plant conditions, the exposure of on-site personnel and population to radiation generated by the primary circuit and associated systems.	DBC-1 DBC-2i DBC-2ii DBC-3i DBC-3ii DBC-4	1, 2, 3, 4, 5, 6a, 6b	A
JMA-R-1333	The Containment Vessel Structure [JMA] shall contain coolant within the Containment Boundary when the Emergency Core Cooling System [JN01] is in operation.	DBC-2ii DBC-3i DBC-3ii DBC-4	1, 2, 3, 4, 5	A

Non-functional performance requirements associated with the safety categorised functional requirements are also being developed and allocated in the DOORS Containment Vessel Structure [JMA] Requirements Modules, including the rationale for their selection, which are not repeated here.

Non-Functional System Requirements

A full set of non-functional system requirements are in development based on the E3S Design Principles, which will be systematically applied to each SSC as part of the systems engineering process. All requirements are subject to refinement and finalisation.

Safety Classification

The Containment Vessel Structure [JMA] is the principal means by which the Category A safety function CoRM is achieved, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2], the safety classification of components within the system is Class 1.

Seismic Classification

The seismic classification of SSCs is still to be assigned in accordance with methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [2].

Description of SSC

The Containment Vessel Structure [JMA] houses the primary circuit, RPV, SGs, pressuriser and associated equipment and safety systems. The primary function of the Containment Vessel Structure [JMA] is to ensure confinement of radionuclides during all normal, fault and accident conditions, thus protecting the outside environment.

The vessel is a leak tight, free-standing steel pressure vessel, 37m high and 31.5m in diameter. It consists of a cylindrical shell and two semi-elliptical domes. The shell and domes are manufactured from SA738 Grade B curved plates approximately 60mm thick.

The lower dome is supported by a thick concrete basemat which is in turn supported off aseismic bearings which are mounted on the Reactor Island foundation slab. The aseismic bearings provide attenuation of horizontal accelerations during an earthquake (described further in E3S Case Chapter 9B: Civil Engineering Works & Structure, Reference [21].

The vessel is designed and substantiated to ASME Section III, Division 1, subsection NE, Class MC Components 2021. The Containment Vessel Structure [JMA] is illustrated in Figure 6.4-1.

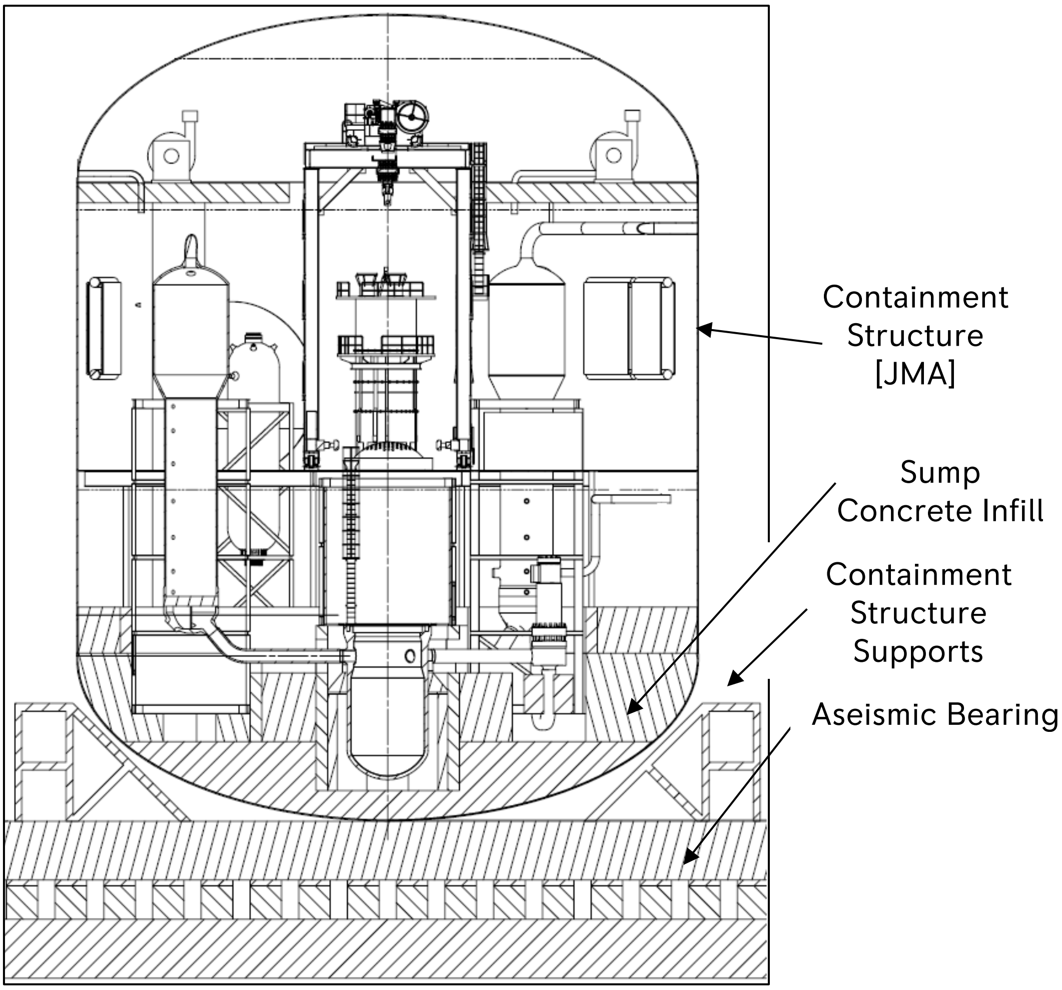


Figure 6.4-1: Containment Vessel [JMA] Schematic

Monitoring, Inspection, Testing & Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of the ASF [JD02] will need to be replaced within that period. An outline maintenance plan for the ASF [JD02] is still to be developed.

Due to the RR SMR duty reactivity being boron-free, maintenance and testing of the ASF [JD02] will be limited to functional tests of distributed parts of sub-systems.

At PCD, a generic verification strategy for the Containment Structure [JMA] to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements are in development and stored in DOORS.

Verification will predominantly be through inspection and analysis, with key risks identified to develop the verification strategy, including the vessel solution being dependent on plant operating conditions and chosen vendor, and trial run of the manufacturing process.

Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 6.0.2. Ongoing design development, optimisation, and maturing requirements has led to a decision to resize the geometry of the Containment Vessel Structure [JMA] to 34.5m diameter and 41.5m high overall. This is expected to be implemented as part of the FCD design baseline.

All design development risks and opportunities are captured and managed by design teams.

6.4.3 Containment Heat Removal Systems

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.4 Systems for Control of Hydrogen in Containment

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.5 Mechanical Features of Containment

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.6 Annulus Ventilation System

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.7 Ventilation System

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.8 Filtered Venting System

Section Placeholder – to be populated in future revisions of the E3S Case

6.4.9 Containment Leakage System

Section Placeholder – to be populated in future revisions of the E3S Case

6.5 Habitability Systems

Section Placeholder – to be populated in future revisions of the E3S Case

6.6 Systems for Removal & Control of Fission Products

Section Placeholder – to be populated in future revisions of the E3S Case

6.7 Conclusions

6.7.1 Conclusions

Preliminary evidence is presented to support the overall chapter Claim that 'RR SMR Engineered Safety Features are designed and substantiated to achieve functional and non-functional safety requirements through the lifecycle and reduce risks 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 SSCs presented in this revision of the E3S Case include the ECCS [JN01], PDHR [JN02], Scram [JD01], ASF [JD02], and Containment Vessel [JMA]. For each SSC, the design definition presented describes how the SSC is being developed to meet its requirements and reduce risks to ALARP, based on its maturity at the PCD design stage. SSCs excluded from this revision based on limited maturity, as listed in Appendix B, will be incorporated as their design is matured.

The full suite of evidence to underpin the Claim will be developed in line with the CAE Route Map and reported in future revisions of the E3S Case, including full traceability of safety categorised requirements from the safety analysis, a complete set of non-functional system requirements from the E3S design principles, further development of the SSC concept design to meet safety requirements, and ultimately substantiation of safety requirements.

6.7.2 Assumptions & Commitments on Future Dutyholder

None identified at this revision.

6.8 References

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

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

[3] RR SMR Report, SMR0004363/001, “E3S Case Chapter 23: Structural Integrity,” March 2023.

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

[5] RR SMR Report, SMR0003023/001, “Rolls-Royce Small Modular Reactor Codes and Standards,” October 2022.

[6] RR SMR Report, SMR0003977/001, “E3S Case Chapter 15: Safety Analysis,” March 2023.

[7] RR SMR Report, SMR0000531, “Rolls-Royce SMR Deterministic Safety Case - Methodologies,” October 2022.

[8] RR SMR Report, SMR0000911/001, “System Description for the Emergency Core Cooling System [JN01],” June 2022.

[9] RR SMR Report, SMR0003984/001, “E3S Case Chapter 5: Reactor Coolant System & Associated Systems,” March 2023.

[10] RR SMR Report, SMR0001055/001, “System Description for the Low Pressure Injection System [JNG],” June 2022.

[11] RR SMR Report, EDNS01000903077/001, “SMR Reactor Island Operating Philosophy,” October 2020.

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

[13] RR SMR Report, SMR0003939/001, “E3S Case Chapter 7: Instrumentation & Control,” March 2023.

[14] RR SMR Report, SMR0004289/001, “E3S Case Chapter 14: Plant Construction & Commissioning,” March 2023.

[15] RR SMR Report, SMR0000624/001, “System Description for the Passive Decay Heat Removal System [JN02],” June 2022.

[16] RR SMR Report, SMR0001230/001, “System Description for the Passive Steam Condensing System [JNB],” June 2022.

[17] RR SMR Report, EDNS01000925748/001, “System Outline Description for the High Pressure Injection System [JND],” January 2021.

[18] RR SMR Report, SMR0000639/001, “System Description for the Scram Function [JD01],” June 2022.

[19] RR SMR Report, SMR0000638/001, “System Description for the Alternative Shutdown Function [JD02],” June 2022.

[20] RR SMR Report, SMR0000637/001, “System Description for the Emergency Boron Injection System [JDK],” June 2022.

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

6.9 Appendix A: CAE Route Map

6.9.1 Chapter 6 Route Map

A preliminary Claims decomposition from the overall Chapter 6 Claim is summarised in Table 6.9-1, including the Tier 2 Evidence underpinning the Claims at PCD (i.e., summarised in Revision 1 of this report) and further Tier 2 Evidence still to be developed.

Table 6.9-1: CAE Route Map

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 6**	**Underpinning Tier 2 Evidence** ***at PCD**	**Underpinning Tier 2 Evidence** ***to be developed**
Safety functional & non-functional system requirements are derived and justified based on sound safety principles and methods	-	-	A comprehensive set of functional requirements are derived in the safety analysis (Fault Schedule), placed on Structures, Systems & Components based on functions to be	Section 6.1.1	JN01-R ECCS DOORS Module	Revised DOORS Requirements Modules for each SSC
				Section 6.1.2	JN02-R PDHR DOORS Module	
				Section 6.2.1	JD01-R Scram DOORS Module	
				Section 6.2.2	JD02-R ASF DOORS Module	

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 6	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
			delivered during Plant States DBC-1 to DBC-5 Non-functional requirements are derived from the E3S principles and applied to the architecture of SSCs in accordance with their classification	Section 6.4.1	JMA-R Containment Module	
Architecture is designed to achieve safety requirements, considering RGP & OPEX to reduce risks to ALARP	-	-	The preferred design solution has been developed following a structured systems engineering approach with evaluation against safety criteria supporting the decision-making process	Section 6.1.1	ECCS System Description [8]	Revised System Descriptions for each SSC
				Section 6.1.2	PDHR System Description [15]	
				Section 6.2.1	Scram System Description [18]	
				Section 6.2.2	ASF System Description [19]	
				Section 6.4.1	Not Applicable (n/a)	

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 6**	**Underpinning Tier 2 Evidence** ***at PCD**	**Underpinning Tier 2 Evidence** ***to be developed**
The design has been substantiated to achieve its safety requirements through the lifecycle	Safety requirements for the design have been verified	-	Verification activities to demonstrate safety requirements can be achieved have been developed based on sound engineering judgement and methods	Section 6.1.1 Section 6.1.2 Section 6.2.1 Section 6.2.2 Section 6.4.1	Verification activities in DOORS Verification Modules	Revised DOORS Verification Modules for each SSC
	Safety requirements have been verified through manufacturing, construction, installation, and commissioning	-	Processes and controls are designed to verify safety requirements during manufacturing, construction, installation, and commissioning	n/a	n/a	Installation and Commissioning Plans for each SSC (TBC)

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 6**	**Underpinning Tier 2 Evidence** ***at PCD**	**Underpinning Tier 2 Evidence** ***to be developed**
	Design can deliver its safety requirements during its operational life	-	The design identifies and facilitates EMIT activities commensurate with its safety classification to demonstrate its status, availability, and integrity in line with the design intent	n/a	n/a	Maintenance Plans for each SSC (TBC)

6.10 Appendix B: SSCs in Scope of Chapter 6

Table 6.10-1 lists those SSCs that are within the scope of Chapter 6, and the section of the report they are addressed.

Table 6.10-1: SSCs in Scope of Chapter 6

RDS-PP	SSC	Section in Chapter 6
JD01	Scram	Section 6.2.1
JD02	Alternative Shutdown Function	Section 6.2.2
JDK	Emergency Boron Injection System	
JM	Reactor plant containment systems	Covered by sections containing [JM_] system codes
JMA	Containment Vessel Structure	Section 6.4
JM01	In-Vessel Retention	Section 6.3.1
JMB	Core Melt Stabilisation System	Not covered in this revision based on low design maturity
JMD	Containment penetration for fuel transfer	
JME	Equipment transfer airlock	
JMF	Personnel airlock	
JMK	Containment mechanical penetrations	
JML	Containment cable penetrations	
JMM	Containment leak monitoring and collection	
JMN	Containment spray	
JMR	Containment venting and filtering	Not covered in this revision based on low design maturity
JMS	Hydrogen mixing	
JMT	Hydrogen reduction	
JMU	Hydrogen monitoring	
JN	Reactor heat removal systems	Covered by sections containing [JN_] system codes
JNM	Reactor vessel cavity injection system	Section 6.3.1
JN01	Emergency Core Cooling System	Section 6.1.1
JNF	Automatic Depressurisation System	

RDS-PP	SSC	Section in Chapter 6
JNG	Low Pressure Injection System	
JN02	Passive Decay Heat Removal System	Section 6.1.2
JNB	Passive steam condensing system	
JND	High Pressure Injection System	
JNK	Local Ultimate Heat Sink system	Section 6.1.1& Section 6.1.2
JN03	Shut Down Decay Heat Removal System	Not covered in this revision based on low design maturity
FAN	Emergency heat removal system for coolant used for storage of spent fuel assemblies	Not covered in this revision based on low design maturity
FCF	Airlock system for fuel assemblies /reactor internals between rooms	Not covered in this revision based on low design maturity
KAX	Safety measure coolant supply subsystem	Not covered in this revision based on low design maturity
KH	Nuclear heat tracing systems	
LJ	Emergency feedwater supply system	Not covered in this revision based on low design maturity
LJA	Emergency feedwater system for nuclear steam generator	
LJB	Emergency feedwater system for nuclear steam generator	
LJC	Emergency feedwater system for nuclear steam generator	
LJD	Emergency feedwater system for nuclear steam generator	

RDS-PP	SSC	Section in Chapter 6
LJK	Emergency feed system on feedwater side of nuclear steam generator	

6.10 Acronyms and Abbreviations

1oo’X’	One out of ‘X’
AIV	Automatic Isolation Valve
ALARP	As Low as Reasonably Practicable
ASF	Alternative Shutdown Function
ASME	American Society of Mechanical Engineers
BoD	Basis of Design
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CDF	Core Damage Frequency
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRM	Confinement of Radioactive Material
CRDM	Control Rod Drive Mechanism
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
DR	Definition Review
DVI	Direct Vessel Injection
E3S	Environment, Safety, Security and Safeguards
EBD	Emergency Blow Down
ECC	Emergency Core Cooling
ECCS	Emergency Core Cooling System
EMIT	Examination, Maintenance, Inspection and Testing
EUR	European Utility Requirements

FCD	Final Concept Definition
FSF	Fundamental Safety Function
GER	Generic Environmental Report
GSR	Generic Security Report
HLSF	High-Level Safety Function
HP	High Pressure
HPIS	High Pressure Injection System
HR	High Reliability
C&I	Instrumentation & Control
IAEA	International Atomic Energy Agency
ICF	Intact Circuit Fault
IVR	In-Vessel Retention
LOCA	Loss of Coolant Accident
LP	Low Pressure
LPIS	Low Pressure Injection System
LUHS	Local Ultimate Heatsink System
LVCS	Level and Volume Control System
MCR	Main Control Room
MSIV	Main Steam Isolation Valve
n/a	Not Applicable
NOP	Normal Operating Pressure
OPEX	Operating Experience
PCC	Passive Containment Cooling
PCD	Preliminary Concept Definition
PCSR	Pre-Construction Safety Report
PDHR	Passive Decay Heat Removal
PIE	Postulated Initiating Event

PSA	Probabilistic Safety Assessment
PSCS	Passive Steam Condensing System
PWR	Pressurised Water Reactor
RCS	Reactor Coolant System
RD	Reference Design
RDS-PP	Reference Designation System for Power Plants
RGP	Relevant Good Practice
RPV	Reactor Pressure Vessel
RR SMR	Rolls-Royce Small Modular Reactor
RVCIS	Reactor Vessel Cavity Injection System
SBO	Station Black Out
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SSC	Structure, System and Component
TBC	To Be Confirmed
VHR	Very High Reliability