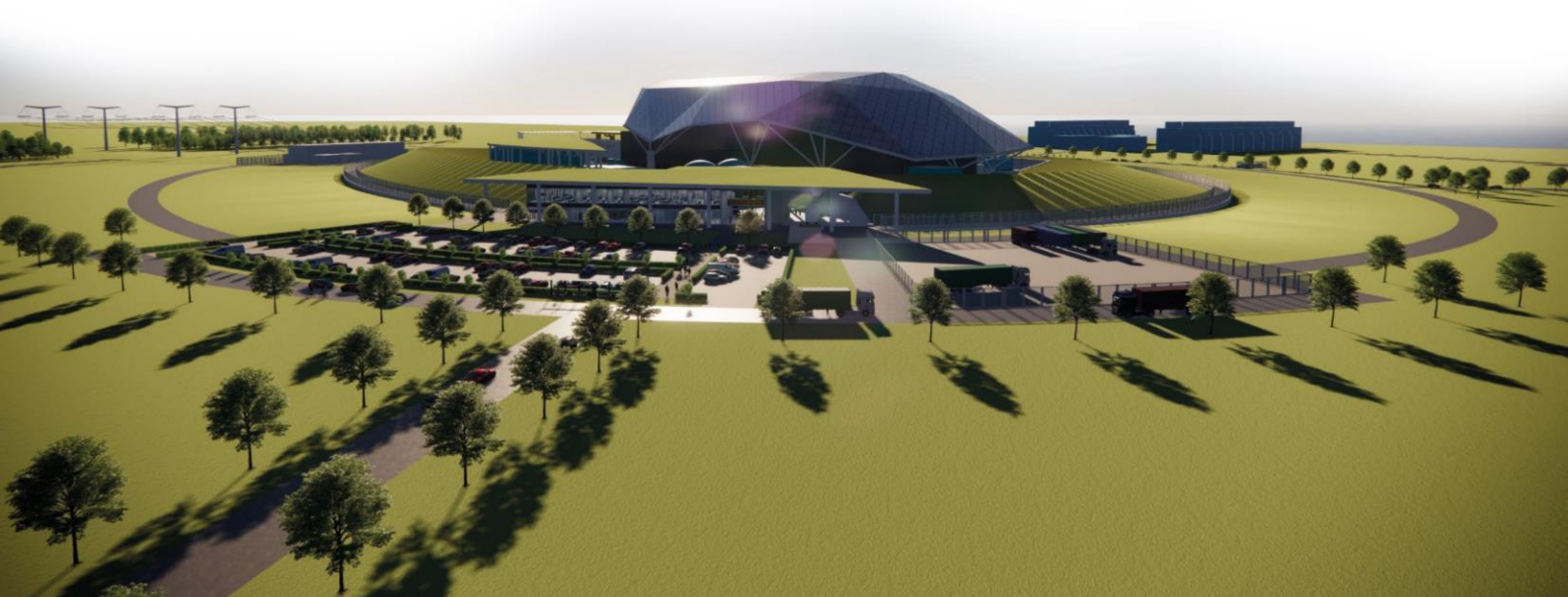
Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 6: Engineered Safety Features



Record of Change

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First issue of E3S Case
March 2024	2	Issue	It incorporates revisions and new design developments of the engineering safety features based on Reference Design 7, aligned to Design Reference Point 1, including: • Additional design definition for all systems included in the first issue • Design definition for the Containment Safety Measure [JM01] and associated sub-systems • Functions and description of the High Temperature Heat Removal [JN03] and Low Temperature Decay Heat Removal [JN04] Safety Measures • Reference to habitability systems
May 2024	3	Issue	Updated to correct revision history status at Issue 2. Chapter changes include: • Additional detail within the conclusions for how arguments and evidence presented meet the generic E3S objective Also minor template/editorial updates for overall E3S Case consistency.

Executive Summary

Chapter 6 of the generic Environment, Safety, Security, and Safeguards (E3S) Case presents the measures and associated structures, systems, and components (SSCs) of the Rolls-Royce Small Modular Reactor (RR SMR) that deliver E3S functions during design basis conditions (DBCs) and design extension conditions (DECs).

The chapter outlines the arguments and evidence to underpin the top-level claim that the RR SMR engineered safety features are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to as low as reasonably practicable (ALARP), apply best available techniques (BAT) and ensure secure by design and safeguards by design.

The measures covered include the Emergency Core Cooling (ECC) [JN01], Passive Decay Heat Removal (PDHR) [JN02], Scram [JD01], Alternative Shutdown Function (ASF) [JD02], and Containment Safety Measure [JM01], as well as associated sub-systems.

For each measure, the safety functions to be delivered by each SSC are presented, with the assignment of safety categorised functional requirements to achieve them. Non-functional system requirements derived from the E3S design principles are also presented. The design definition presented for each system is developed based on relevant good practice (RGP) and operating experience (OPEX). It is developed and evaluated in accordance with the E3S design principles through the integrated E3S and engineering processes, including design to codes and standards according to the safety classification, down-selection of options in accordance with criteria to ensure risks are reduced to ALARP, apply BAT, and are secure by design and safeguards by design, and confirmatory performance analysis. This provides confidence that claims can be met when the full suite of arguments and evidence is developed. No functional requirements for environment, security and safeguards are identified for the SSCs within the scope of this chapter.

Version 2 of the generic E3S Case is developed in support of the reference design 7 (RD7) design, corresponding to design reference point 1 (DRP1) for the generic design assessment (GDA). Further arguments and evidence are to be developed to underpin the top-level claim, including continued iterative E3S analysis and finalisation of E3S requirements, detailed design development of all SSCs, and verification and validation of E3S 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 presents the overarching summary and entry point to the design and E3S information for the RR SMR measures and associated structures, systems, and components (SSCs) that deliver E3S functions during design basis conditions (DBCs) (fault conditions) and design extension conditions (DECs) at defence in depth levels 3 and 4.

6.0.2 Scope and Maturity

The list of SSCs that are included in the scope of this chapter is provided in Appendix B (Section 6.10).

The scope of this chapter covers the design definition for each SSC, including allocation of E3S requirements and E3S categorisation and classification, design description, and verification and validation (V&V) activities. It covers the mechanical design aspects, however the selection of materials and justification of the integrity of SSCs is covered in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

All E3S requirements that are assigned to SSCs within this chapter follow the methods described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2]. Safety categorised functional requirements are aligned to delivery of the fundamental safety functions (FSFs), control of fuel temperature (CoFT), control of reactivity (CoR), confinement of radioactive material (CoRM) and control of radiation exposure (CoRE). FSFs are decomposed into high-level safety functions (HLSFs) in the fault schedule and flow to SSCs; the demonstration that HLSFs can be achieved for bounding fault sequences is presented in detail in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

Version 2 of the generic E3S Case is based on reference design 7 (RD7), corresponding to design reference point 1 (DRP1) for the generic design assessment (GDA). At RD7/DRP1, the safety functions to be delivered by each SSC are presented, with the assignment of safety categorised functional requirements to achieve them. No functional requirements for environment, security and safeguards are identified for SSCs in the scope of chapter 6 at RD7/DRP1, noting SSCs are designed in accordance with E3S and engineering processes that include development against principles for environment, security, and safeguards. The design definition presented is based on the design maturity of each respective SSC at RD7/DRP1. V&V activities for SSCs are presented and will be developed and undertaken through detailed design.

6.0.3 Claims, Arguments, Evidence Route Map

The overall approach to claims, arguments, evidence (CAE) and the set of fundamental E3S claims to achieve the E3S fundamental objective are described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [4]. The associated chapter level claim for E3S Case Version 2, Tier 1, Chapter 6: Engineered Safety Features is:

Claim 6: Engineered Safety Features are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with secure-by-design and safeguards-by-design

A decomposition of this claim into sub-claims and mapping to the relevant Tier 2 and Tier 3 information containing the detailed arguments and evidence, is presented in the E3S Case Route Map [5]. Given the evolving nature of the E3S Case alongside the maturing design, the underpinning arguments and evidence may still be developed in at detailed design; the trajectory of this information, where possible, is also illustrated in the route map.

A proportionate summary of the arguments and evidence from lower tier information, available at the current design stage, is presented within this chapter. A mapping of the claims to the corresponding sections that summarise the arguments and/or evidence is provided in Appendix A (section 6.9).

6.0.4 Applicable Regulations, Codes and Standards

The SSCs summarised in this chapter are designed in accordance with the E3S design principles [6], which are developed based on United Kingdom (UK) and international regulations, guidance, and practices, as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

The mechanical systems and components summarised in this chapter are designed in accordance with their safety classification. Relevant codes and standards are identified in Table 6.0-1.

Table 6.0-1: Mechanical Design Codes and Standards

Safety Classification	**Design Basis Code**
VHR	American Society of Mechanical Engineers (ASME) III (Sub-section NB) and beyond code requirements
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 and Residual Heat Removal Systems

6.1.1 Emergency Core Cooling

6.1.1.1 System and Equipment Functions

The function of the Emergency Core Cooling (ECC) [JN01] is to remove residual heat from the reactor core during faulted operation and transfer the heat to the atmosphere. The ECC [JN01] safety measure provides the FSF of CoFT in response to both frequent and infrequent faults.

ECC [JN01] relies upon different sets of SSC to provide CoFT following different postulated initiating events (PIEs). These are referred to as 'variants' of the ECC [JN01] safety measure within the fault schedule. The variants of ECC [JN01] and their associated SSC defined at RD7/DRP1 include:

- ECC [JN01] variant 1 – Passive Containment Cooling (PCC) and Local Ultimate Heat Sink (LUHS) [JNK]:
    - LUHS [JNK] for temperature control
    - Automatic Depressurisation System (ADS) [JNF] and Low Pressure Injection System (LPIS) [JNG] for inventory and pressure control
- ECC [JN01] variant 2 – low pressure (LP) ECC:
    - LUHS [JNK] for temperature control
    - ADS [JNF] LP only and LPIS [JNG] for inventory and pressure control
- ECC [JN01] variant 3 – depressurised ECC:
    - LUHS [JNK] for temperature control
    - ADS [JNF] LP only and LPIS [JNG] gravity drain and recirculation only for inventory and pressure control

6.1.1.2 Design Basis

6.1.1.2.1 Functional Requirements

Safety categorised functional requirements specified for the ECC [JN01] based on the HLSFs they deliver are presented in Table 6.1-1 based on [7].

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

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JN01-R-1434	When relevant faults occur Emergency Core Cooling [JN01] (variant 1, with PCC and LUHS) SHALL removal residual heat.	1 to 4a	A

ECC [JN01] provides the principal means of CoFT during intermediate break (IB) and large break (LB) loss of coolant accidents (LOCAs). ECC [JN01] is required as the secondary means of decay heat removal, following subsequent failure of High Temperature Decay Heat Removal (HTDHR) [JN03] and Passive Decay Heat Removal (PDHR) [JN02]. The relevant PIEs that the ECC [JN01] is claimed against are listed in [7].

The safety categorised functional requirements for the ECC [JN01] are flowed down and allocated to relevant sub-systems and/or components in [8]. Non-functional performance requirements associated with the safety categorised functional requirements are allocated in [7].

No environment, security or safeguards functional requirements are assigned at RD7/DRP1.

6.1.1.2.2 Non-Functional System Requirements

Non-functional system requirements are allocated to the ECC [JN01] based on the E3S design principles as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2], summarised in Table 6.1-2.

Table 6.1-2: ECC [JN01] Non-Functional System Requirements

Requirement ID	Non-Functional System Requirement
JN01-R-1609	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.
JN01-R-1667	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.
JN01-R-2170	Safety measures shall deliver the defined success criteria.
JN01-R-1528	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the presence of a single failure.
JN01-R-1660	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the worst normally permitted configuration of equipment outages for maintenance, test, or repair.
JN01-R-1663	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.

Requirement ID	Non-Functional System Requirement
JN01-R-1662	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.
JN01-R-2171	The design shall fail to a safe state where practicable
JN01-R-1661	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions with diverse means of initiation to the extent reasonably practicable, which shall be via the use of different variables, when the measure requires automatic initiation.
JN01-R-1676	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.
JN01-R-1636	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the main control room (MCR) within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.
JN01-R-1435	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.
JN01-R-1680	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.
JN01-R-1531	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.

6.1.1.2.3 E3S Classification

Safety Classification

The ECC [JN01] is the principal means by which the safety category A function is achieved, and in accordance with the E3S categorisation and classification methodology outlined in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2], the safety classification of components within the system is safety class 1.

Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

Seismic Performance Classification

The seismic performance classification will principally be SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.1.1.3 Description

The baseline architecture for ECC [JN01] consists of three cooling trains, each aligned to the Reactor System [JA]. Decay heat is transferred to the atmosphere via depressurisation of the Reactor Coolant System (RCS) [JE] and sustained injection of coolant via gas pressurised accumulators, gravity drain and sump recirculation. Pressure blowdown is provided by the ADS [JNF] and Reactor System [JA] injection is provided by the LPIS [JNG]. Ultimate heat removal from the Containment System [JMA] atmosphere is provided by the LUHS [JNK], which supplies coolant from the LUHS tanks to the PCC heat exchangers within containment. Steam is generated in the PCC heat exchanger, before returning to the LUHS tanks and vented to atmosphere.

ECC [JN01] places E3S requirements on many other SSCs in support of decay heat removal. Key systems that support ECC [JN01], in addition to those above, include the Refuelling Pool [FAF] for coolant storage, the Containment Lower Dome Civil Structure [UJA20] for maintaining flood-up level and the Containment System [JMA] for inventory control during sump recirculation.

The system architecture can be separated into three phases based on the transient progression following ECC [JN01] initiation, each described below.

Phase 1 – Blowdown and Accumulator Injection

On initiation of ECC [JN01], blowdown valves within the three High Pressure (HP) ADS [JNF] lines open, allowing the contents of the pressurised RCS [JE] to blowdown to the Refuelling Pool [FAF], rapidly reducing plant pressure.

Each HP ADS [JNF] line includes an Emergency Blow Down (EBD) valve which prevents spurious depressurisation as a result of Reactor Control and Protection System [JY] failure. It also includes a multi-stage control valve (MSCV), which opens gradually to minimise mechanical and thermal transients, and a sparge head that distributes steam within the Refuelling Pool [FAF] reducing the mass of steam discharged to the containment atmosphere. Each HP ADS [JNF] line is sized to deliver RCS [JE] depressurisation in event that the other two lines are unavailable.

Three LPIS [JNG] accumulators, located in the Interspace [UJB], are each filled with water and pressurised with nitrogen. When the reactor circuit depressurises to below the accumulator pressure, the water from the accumulators will be forced into the Reactor System [JA] via three direct vessel injection (DVI) nozzles, re-flooding the Reactor Vessel [JAA]. Each of the three accumulator injection lines is configured to provide the minimum reflood flowrate and volume required.

Phase 1 is considered complete when the accumulators are depleted, and in the case of large LOCA, the coolant mixture level exceeds the level of the heated Fuel Assemblies [JAK].

Phase 2 – Gravity Drain

Initiation of LP ADS signals the transition to phase 2. Upon detection of accumulator low low level, the accumulators are isolated from the Reactor System [JA] and three LP ADS [JNF] lines open, allowing steam collected in the outlet plenum to vent to the containment atmosphere. When the accumulators have discharged and plant pressure has equalised with containment, a continuous supply of coolant is provided via three LPIS [JNG] gravity drain lines which connect the elevated Refuelling Pool [FAF] to the DVI nozzles. Each train of gravity drain injection and steam discharge pipework is independently sized to ensure the core remains covered during established gravity drain.

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 System [JMA] as steam via the blowdown line and is collected in the containment sump. Steam via a potential leak (from the initiating event itself) can also condense on the PCC heat exchangers and collect in the containment sump.

Phase 2 is considered complete at the point at which the Refuelling Pool [FAF] level is equal to the coolant level within the containment sump.

Phase 3 – Recirculation

Recirculation lines allow coolant collected in the containment sump to be transferred from the containment sump to the Reactor System inlet plenum via the LPIS [JNG] strainers and DVI nozzles. 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 meet the ECC acceptance criteria.

Steam generated in the Reactor System [JA] throughout the transient is discharged via a low-pressure blowdown line to the Containment System [JMA]. The LUHS [JNK] 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. Each LUHS [JNK] train is sized to provide 24 hours of heat removal; 2oo3 LUHS [JNK] trains are sufficient to provide 72 hours of heat removal and 3oo3 LUHS [JNK] trains are sufficient to provide at least 120 hours of heat removal. Upon detection of LUHS low level, the tanks' inventory can be replenished from other on-site water sources.

The baseline key performance and design parameters for ECC [JN01] are presented in Table 6.1-3. A simplified schematic of the key SSC contributing to ECC [JN01] operation is illustrated in Figure 6.1-1.

Table 6.1-3: Key Performance and Design Parameter for ECC [JN01]

Parameter		**Value**
Phase 1 Blowdown And Accumulator Injection	Accumulator injection pressure	{REDACTED}
	Accumulator water volume	{REDACTED}
	Accumulator gas volume	{REDACTED}
	Injection duration	{REDACTED}
	Accumulator redundancy	1oo3
Phase 2 Gravity Drain	Maximum injection flowrate	{REDACTED}
	Injection duration	{REDACTED}
	Injection line redundancy	1oo3
	Maximum injection flowrate	{REDACTED}

Parameter		Value
Phase 3 Sump Recirculation	Injection duration	Until plant recovery
	Injection line redundancy	1oo3
Containment Heat Removal	PCC heat exchanger duty	{REDACTED}
	Containment design pressure	{REDACTED}
	LUHS boil-off inventory	{REDACTED} (per train)
	LUHS redundancy	1oo3 (24 hrs) 2oo3 (72 hrs)

The ECC [JN01] allocates E3S requirements to a range of SSCs that deliver its functions, described further in [9], including:

- ADS [JNF]
- LPIS [JNG]
- LUHS [JNK]
- Refuelling Pool [FAF]
- Reactor System [JA]
- Reactor Coolant Pressure Relief System [JEG]
- Containment System [JMA]
- Reactor Control and Protection System [JY]
- Main Steam System [LBA] (specifically the piping and main steam isolation valves (MSIVs) on Reactor Island [LBA20])
- Main Feedwater System [LAB] (specifically the piping and feedwater isolation valves on Reactor Island [LAB20])
- Steam Generator Relief System [LBK10]
- Containment Lower Dome Civil Structures [UJA20]

It is noted that the Main Steam System [LBA] and the Main Feedwater System [LAB], described in E3S Case Chapter 10: Steam and Power Conversion Systems [10], span across both Reactor Island and Turbine Island. The ECC [JN01] places safety category A functions onto the Reactor Island parts of the system.

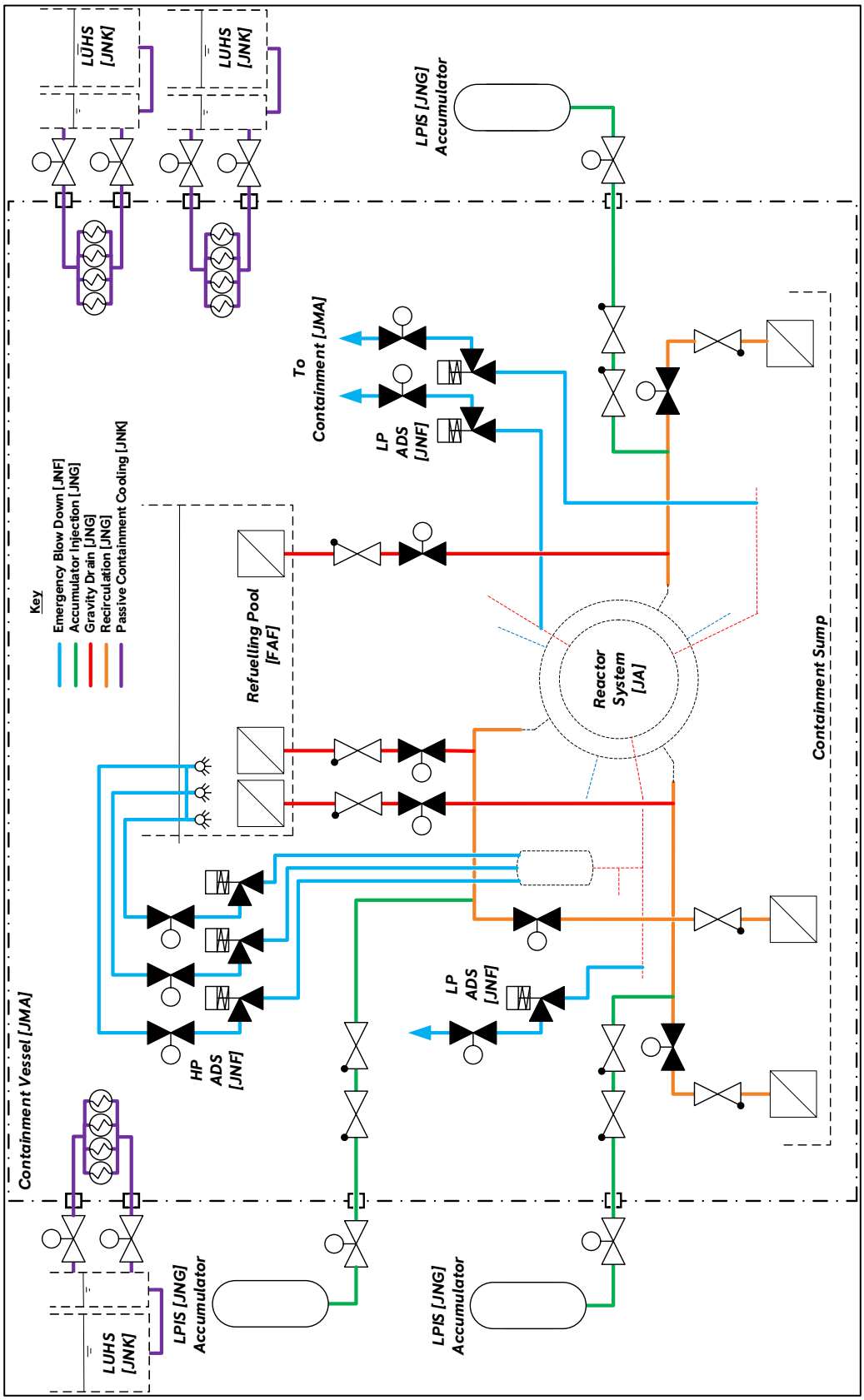


Figure 6.1-1: Simplified Schematic of ECC [JN01]

The developing layout of SSCs supporting ECC [JN01] operation is summarised in [11]. Each of the key sub-systems delivering the ECC [JN01] are located within the hazard shield and on the aseismic bearing to provide protection against external hazards.

Separation and segregation of redundant trains is adopted within the layout to ensure the ECC [JN01] can deliver its function in the event of an internal hazard, examples include:

- Three DVI nozzles are positioned equidistant around the Reactor Pressure Vessel (RPV) [JAA]
- Each train of LP ADS [JNF] pipework is connected to an RCS [JE] hot leg
- The LPIS [JNG] accumulators are spatially segregated and contained within the buttresses of the Interspace [UJB] in the northeast, northwest, and southeast corners. Each accumulator is located below a coupled LUHS [JNK] tank. The 1oo3 redundancy arrangement of the accumulators and coupled LUHS [JNK] tanks allow each interspace buttress to provide segregation between interspace corners, meaning an internal blast from an accumulator can only damage a single train of the LUHS heat removal pathway.

Further description of the ECC [JN01] safety measure, including detail of the associated sub-systems and components, is provided in the ECC Safety Measure Design Description (SMDD) [9].

6.1.1.4 Materials

The description and justification of materials used for safety class 1 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.1.1.5 Interfaces with Supporting Systems

The ECC [JN01] is required to function in conjunction with Scram [JD01] for CoR, described in section 6.2.1.

The ECC [JN01] is automatically initiated by the control & instrumentation (C&I) system, specifically the Reactor Control and Protection System [JY], see section 6.1.1.7.

The ECC [JN01] is designed to avoid active operations that require continuous AC power. DC power demands are limited to actuators and associated with initiation of ECC [JN01]. These power demands are supplied from the grid or Main Generator [MK] (house load operation), or where these are unavailable, supplied from the Low Voltage Uninterruptible DC Supply System for Safety Services [BQ], described further in E3S Case Chapter 8: Electrical Power System [12].

6.1.1.6 System and Equipment Operation

6.1.1.6.1 Normal Operation

The Reactor Island Operating Philosophy [13], 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 Version 2, Tier 1, Chapter 13: Conduct of Operations [14].

During operating mode 1 (power operation), the ECC [JN01] is maintained in a standby state. During operating mode 2 (low power) the control rods are withdrawn in the core and the steam generators

(SGs) are aligned to their power operations configuration. During operating mode 3 (hot standby), the reactor will be shutdown and High Temperature Heat Removal (HTHR) [JN03] will be the default means of heat removal, with ECC [JN01] in standby.

During operating mode 4a (Hot Shutdown – Steaming), reactor coolant temperature and pressure will be reduced from normal operating temperature (NOT) and normal operating pressure (NOP) to approximately {REDACTED} respectively. Conversely, during start-up, reactor coolant temperature will be raised from {REDACTED} to NOT and NOP respectively. The rate of plant pressure reduction is controlled via spray throttling, to maintain a margin of {REDACTED} between hot leg saturation pressure and plant pressure. Although plant pressure is reduced below operating mode 1 operating conditions, the use of cold leg saturation condition as a means of automatic initiation allows ECC [JN01] to continue in standby.

During operating mode 4b (hot shutdown – non-steaming), reactor coolant temperature and pressure will be reduced from 120 °C and 2.0 MPa(a) to approximately 93 °C and 1.0 MPa(a) respectively. Conversely during start-up, reactor coolant temperature and pressure will be increased from approximately {REDACTED}. RCS [JE] pressure will remain relatively constant at {REDACTED}. HP ADS [JNF] is no longer required therefore ECC variant 2 is in standby (see section 6.1.1.1).

During operating mode 5a (cold shutdown – pressurised), reactor coolant temperature and pressure will be reduced from {REDACTED} below {REDACTED} and to atmospheric pressure. Conversely during start-up, reactor coolant temperature and pressure will be increased from {REDACTED} and atmospheric pressure to approximately {REDACTED}respectively. HP ADS [JNF] is no longer required therefore ECC variant 2 is in standby (see section 6.1.1.1).

During operating mode 5b (cold shutdown – depressurised), the plant is fully depressurised and coolant temperature is maintained as low as possible by the Cold Shutdown Cooling System (CSCS) [JNA]. Neither HP ADS [JNF] or accumulator injection are required therefore ECC variant 3 is in standby (see section 6.1.1.1).

During operating mode 6a (refuelling with reduced water level above fuel), the RCS [JE] is drained in preparation for removal of the Reactor System [JA] Integrated Head Package (IHP). ECC [JN01] is expected to remain available via operator initiation.

During operating mode 6B (refuelling with water level above fuel at nominal full), the refuelling cavity is flooded to facilitate fuel movement. ECC [JN01] is expected to remain available via operator initiation.

The component configuration for ECC [JN01] in standby during all normal operating modes are listed in [9].

6.1.1.6.2 Operation during Faults

Following all PIEs in operating mode 1, successful scram is required to shutdown the reactor as a precursor to enable successful ECC operation.

Decay heat removal after reactor shutdown will be provided by HTHR [JN03] when a heat removal path from the SGs to the condenser or Atmospheric Steam Dump (ASD) [LBK50] is available. If the condenser is unavailable, then decay heat removal can be provided for several hours via SG bleed and feed, where the main feed or auxiliary feed pumps supply feedwater to the SGs and the ASD [LBK50] provides a bleed path to the environment.

If all feed is unavailable, then PDHR [JN02] is the first CoFT protective safety measure. If PDHR [JN01] is unavailable, then ECC [JN01] is the final CoFT protective safety measure in design basis conditions (DBCs).

No operator action is required to control temperature during the first 72 hours of ECC [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 System [JMA], it is necessary to isolate the containment vessel and connected systems on initiation of the ECC [JN01]. This automatic isolation includes isolation of all containment fluid penetrations, excluding the accumulators and PCC connection to the LUHS [JNK].

After a prolonged period of ECC [JN01] operation (>72 hours), the LUHS [JNK] level could fall to such an extent that further water is required to continue reactor cooling. The operator can observe the fall in LUHS [JNK] level from the MCR; if available, they can drain the contents of the third LUHS [JNK] tertiary tank into the active LUHS [JNK] train(s) or the operator will need to align further water supplies to the spare fill line in the active LUHS [JNK] tertiary tank(s).

Specific operational responses to fault conditions are described in [9].

6.1.1.7 Instrumentation and Control

All ECC [JN01] functionality can be automatically initiated without reliance on the operator for at least 72 hours following all PIEs. This is achieved through a series of automatic control and instrumentation functions, described in [9].

The ECC [JN01] can be initiated by both the Reactor Protection System (RPS)1 [JRA10] and Diverse Protection System (DPS) [JQA] within the Reactor Control and Protection System [JY], depending on the first plant parameter which is met. The Reactor Control and Protection 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 supplementary control room (SCR). It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits.

The Reactor Control and Protection System [JY] and allocation of safety categorised functional requirements from the ECC [JN01] is described further in E3S Case Version 2, Tier 1, Chapter 7: Instrumentation & Control [15].

6.1.1.8 Monitoring, Inspection, Testing & Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of the ECC [JN01] will need to be replaced within that period.

The examination, maintenance, inspection and testing (EMIT) activities for the ECC [JN01] are defined as through-life activities (TLA) within the RR SMR requirements management database, and cover safety derived tasks (in-service inspection (ISI)), reliability derived tasks (reliability centred maintenance (RCM)/preventative maintenance), and industry best practice/operational experience (OPEX) (Electrical Power Research Institute (EPRI) Preventative Maintenance Basis Database (PMBD)).

6.1.1.9 Radiological Aspects

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

ECC [JN01] is required in response to initiating events, such as Steam Generator Tube Rupture (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]. Radiological consequences for fault sequences are described further in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.1.1.10 Performance and Safety Evaluation

6.1.1.10.1 Compliance with Safety Categorised Functional Requirements

Verification strategies for the ECC [JN01] to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements primarily include performance analysis using RELAP5-3D and GOTHIC codes, with thermal-hydraulic rig testing to validate analysis.

Performance analysis demonstrates that the ECC [JN01] successfully removes heat to deliver its safety function for all fault conditions at RD7/DRP1. The output of performance analysis and margin to acceptance criteria for the ECC [JN01] are presented in [9], with the suite of performance analysis for bounding fault conditions that place safety categorised functional requirements on the ECC [JN01] presented in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.1.1.10.2 Compliance with Non-Functional System Requirements

A summary of the compliance for non-functional system requirements allocated to the ECC [JN01] are summarised in Table 6.1-4. Further details are provided in [7] and [9].

Table 6.1-4: ECC [JN01] Non-Functional System Requirements Compliance

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN01-R-1609	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.	ECC [JN01] is designed with three redundant trains which are segregated such that a single internal hazard in unlikely to result in common cause failure (CCF) of more than one train of ECC [JN01].

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN01-R-1667	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.	All Class 1 SSCs which support ECC [JN01] are contained within and supported upon the Hazard Shield and Aseismic Bearing respectively. ECC [JN01] is designed with three redundant trains which are segregated such that a single external hazard in unlikely to result in CCF of more than one train of ECC [JN01].
JN01-R-2170	Safety measures shall deliver the defined success criteria.	Performance analysis demonstrates that the ECC [JN01] successfully removes heat to deliver its safety function
JN01-R-1528	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the presence of a single failure.	ECC [JN01] is designed with three redundant trains with redundancy requirements allocated to all SSCs which support the safety measure.
JN01-R-1660	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the worst normally permitted configuration of equipment outages for maintenance, test, or repair.	The design intent of the Rolls-Royce SMR is that no planned EMIT is required on passive safety systems during normal operations.
JN01-R-1663	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.	ECC [JN01] is designed with three redundant trains with redundancy requirements allocated to all SSCs which support the safety measure. ECC [JN01] is functionally diverse to the PDHR [JN02] CoFT safety measure.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN01-R-1662	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.	ECC [JN01] is designed to deliver its functions in response to the most onerous initial operating states. Performance analysis which support safety measure design use a combined approach including a best-estimate analysis method with conservative assumptions, including initial and boundary conditions.
JN01-R-2171	The design shall fail to a safe state where practicable	Valves that move position in response to a safety demand from the C&I systems or are in pipework that supports successful ECC [JN01] operation, are specified to fail to a safe position upon loss of power. Sensors fail to a trip state, which places the associated RPS/DPS logic train into a tripped state.
JN01-R-1661	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions with diverse means of initiation to the extent reasonably practicable, which shall be via the use of different variables, when the measure requires automatic initiation.	Diverse means of automatic initiation are provided.
JN01-R-1676	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.	For each bounding design basis fault, the ECC [JN01] ensures selected trip parameters relate directly to the fault, where practicable, in order to provide rapid response.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN01-R-1636	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.	For all design basis fault conditions, the ECC [JN01] Safety Measure initiates automatically without operator action.
JN01-R-1435	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.	The design of the ECC [JN01] ensures no essential services are needed from on-site mobile equipment for 72 hours. After a prolonged period of ECC [JN01] operation (>72 hours), the LUHS [JNK] level could fall to such an extent that further water is required to continue reactor cooling. Long-term cooling for the ECC [JN01] solutions is being designed to ensure no essential services are needed from off-site for 7 days.
JN01-R-1680	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.	The ECC [JN01] is designed to interface with offsite equipment in deliver of its categorised functions, primarily via external top up lines to the LUHS [JNK].
JN01-R-1531	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.	Human factors assessment ensure integration through the design process, including human factors checklists, allocation of function, task analysis and human reliability analysis.

6.1.1.10.3 ALARP, BAT, Secure by Design and Safeguards by Design

Key ECC [JN01] design decisions made with respect to ensuring overall risks are reduced to as low as reasonably practicable (ALARP), best available techniques (BAT), secure by design and safeguards by design include:

- Selection of DVI and 1oo3 redundancy for the accumulator architecture, and 1oo3 redundancy for the phase 2 gravity drain lines, based on relevant good practice (RGP) for improved single failure tolerance over 2oo3 designs, and minimising reliance on structural integrity arguments for RCS pipework.

- Use of passive EBD valves on the ADS [JNF] lines to provide functional diversity and protection against spurious blowdown due to C&I failure. Further details of the innovative design of the EBD valves are provided in [9].

- Selection of the Refuelling Pool [FAF] as the LOCA water source rather than a separate water source within containment, which would significantly increase layout complexity and number of components.

- Sharing of the LUHS [JNK] cooling capability between both the ECCS [JN01] and PDHR [JN02] protective safety measures. Further heatsink diversity and risk reduction are incorporated into the design of the RR SMR through the provision of ASD [LBK50]. 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 can achieve suitable levels of defence in depth and achieving numerical targets.

More detailed information on design decisions is presented in the ECC SMDD [9] and associated design decision files.

6.1.2 Passive Decay Heat Removal

6.1.2.1 System and Equipment Functions

The function of the PDHR [JN02] is to remove residual heat from the reactor core and transfer the heat to the atmosphere. The PDHR [JN02] safety measure provides the FSF of CoFT in response to frequent and infrequent faults for which it is claimed.

PDHR [JN02] relies upon different sets of SSC to provide CoFT following different PIEs. These are referred to as 'variants' of the PDHR [JN02] safety measure within the fault schedule. The variants of PDHR [JN02] and their associated SSC defined at RD7/DRP1 include:

- PDHR [JN02] variant 1 – intact circuit fault (ICF):
    - Primary heat removal: pumped or natural circulation (NC)
    - Secondary heat removal: Passive Steam Condensing System (PSCS) [JNB]
    - Tertiary heat removal: LUHS [JNK]
    - Primary inventory and pressure control: High Pressure Injection System (HPIS) [JND]
- PDHR [JN02] variant 2 – LOCA:
    - Primary heat removal: pumped or NC
    - Secondary heat removal: PSCS [JNB]
    - Tertiary heat removal: LUHS [JNK]
    - Primary inventory and pressure control: HPIS [JND]

- Secondary inventory and pressure control: ASD [LBK50] + RCS [JE] connecting system isolation (Chemical and Volume Control System (CVCS) [KB] and Nuclear Sampling System [KUA])

- PDHR [JN02] variant 3 – station blackout (SBO), main steam line break (MSLB) and excessive HPIS make-up:
  - Primary heat removal: pumped or NC
  - Secondary heat removal: PSCS [JNB]
  - Tertiary heat removal: LUHS [JNK]
  - Primary inventory and pressure control: LPIS [JNG] accumulators
  - Secondary inventory and pressure control: ASD [LBK50]
- PDHR [JN02] variant 4 – SGTR:
  - Primary heat removal: pumped or NC
  - Secondary heat removal: PSCS [JNB] and ASD [LBK50] (non-casualty SGs only)
  - Tertiary heat removal: LUHS [JNK]
  - Primary inventory and pressure control: HPIS [JND]
  - Secondary inventory and pressure control: ASD [LBK50].

6.1.2.2 Design Basis

6.1.2.2.1 Functional Requirements

Safety categorised functional requirements specified for the PDHR [JN02] based on the HLSFs they deliver are presented in Table 6.1-5 based on [16].

Table 6.1-5: PDHR [JN02] Safety Categorised Functional Requirements

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JN02-R-1720	When relevant faults occur, Passive Decay Heat Removal [JN02] Variant 1 (ICF) SHALL remove residual heat.	1 to 4a	B
JN02-R-1724	When relevant faults occur, Passive Decay Heat Removal [JN02] Variant 2 (LOCA) SHALL remove residual heat.	1 to 4a	B
JN02-R-1725	When relevant faults occur, Passive Decay Heat Removal [JN02] Variant 3 (SBO, MSLB & Excessive HPIS Make-Up) SHALL remove residual heat.	1 to 4a	C

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JN02-R-1726	When relevant faults occur, Passive Decay Heat Removal [JN02] Variant 4 (SGTR) SHALL remove residual heat.	1 to 4a	B

PDHR [JN02] variants 1, 2 and 4 provide diverse means of providing heat removal for frequent faults and therefore the functions they perform are safety category B (with ECC [JN01] providing the safety category A heat removal function). PDHR [JN02] variant 3 provides a diverse means of providing heat removal following a 24 hr / 168 hr loss of offsite power (LOOP) with a subsequent loss of standby AC power, i.e. SBO. This is an infrequent fault therefore ECC [JN01] provides the principal safety category A heat removal function with the PDHR [JN02] variant 3 heat removal function available as a back-up and is therefore assigned safety category C. The relevant PIEs that the PDHR [JN02] is claimed against are listed in [16].

The safety categorised functional requirements for the PDHR [JN02] are flowed down and allocated to relevant sub-systems and/or components in [17]. Non-functional performance requirements associated with the safety categorised functional requirements are allocated in [16].

No environment, security or safeguards functional requirements are assigned at RD7/DRP1.

6.1.2.2.2 Non-Functional System Requirements

Non-functional system requirements are allocated to the PDHR [JN02] based on the E3S design principles as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2], summarised in Table 6.1-6.

Table 6.1-6: PDHR [JN02] Non-Functional System Requirements

Requirement ID	Non-Functional System Requirement
JN02-R-2111	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.
JN02-R-2112	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.
JN02-R-2119	Safety measures shall deliver the defined success criteria.
JN02-R-1997	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
JN02-R-1996	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.
JN02-R-1978	The design shall fail to a safe state where practicable

Requirement ID	Non-Functional System Requirement
JN02-R-2009	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.
JN02-R-2003	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.
JN02-R-2004	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.
JN02-R-2011	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.
JN02-R-2572	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.

6.1.2.2.3 E3S Classification

Safety Classification

The PDHR [JN02] is the principle means by which the safety category B function is achieved (with the exception of variant 3 which delivers a safety category C function) and in accordance with the E3S categorisation and classification methodology outlined in E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2], the safety classification of components within the system is safety class 2. It is noted that some components, including the accumulators and LUHS tanks, also provide support to the ECC [JN01] (see section 6.1.1) and therefore are safety class 1.

Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

Seismic Performance Classification

The seismic performance classification will principally be SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.1.2.3 Description

The baseline architecture for the PDHR [JN02] safety measure comprises three cooling trains, each aligned to an RCS [JE] loop. Decay heat is transferred from the Fuel Assemblies [JAK] to RCS [JE] coolant, by either reactor coolant pump (RCP) induced flow or, in the event of a loss of pumped flow, NC from the Reactor System [JA] to the RCS [JE].

The RCS [JE] is configured to provide a large thermal driving head between the core and the SGs such that each of the three RCS [JE] loops can remove the maximum required duty under NC flow. Heat is transferred from the reactor coolant to lower pressure secondary coolant plant, via the SG tube walls, which boils to generate pressurised steam.

To support PDHR [JN02] heat removal, the SGs are isolated from the wider steam and feed systems, primarily through closing the MSIVs and feedwater isolation valves. Steam generated within each SG therefore flows out of the SG into the Main Steam System [LBA] and then onwards through PSCS [JNB] pipework to the PSCS [JNB] heat exchangers located within, and cooled directly by, a corresponding water volume in the LUHS [JNK].

The coolant condensed within the PSCS [JNB] heat exchangers falls by gravity through PSCS [JNB] drain lines into the Main Feedwater Water System [LAB] and to the SGs for recirculation. Heat is transferred from the PDHR [JN02] heat exchangers to coolant within the LUHS [JNK] coupled tanks. As heat is transferred, water in the LUHS [JNK] coupled tanks heats up and boils off to atmosphere. LUHS [JNK] tertiary tanks replenish, by gravity, the inventory lost from the LUHS [JNK] coupled tanks during PDHR [JN02] operation.

The three cooling trains of the PDHR [JN02] are independent and configured such that each RCS [JE] / PSCS [JNB] / LUHS [JNK] cooling train is sized to provide heat removal with 1oo3 redundancy. Each LUHS [JNK] train has sufficient stored water to provide 24 hours of heat removal; 2oo3 LUHS [JNK] trains are sufficient to provide 72 hours of heat removal and 3oo3 LUHS [JNK] trains are sufficient to provide at least 120 hours of heat removal.

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:

- Level and Volume Control System (LVCS) [KBA] (details of this system are provided in E3S Case Version 2, Tier 1, Chapter 5: Reactor Coolant System and Associated Systems [18])
- HPIS [JND] should the LVCS [KBA] be unavailable
- LPIS [JNG] should the LVCS [KBA] and HPIS [JND] be unavailable, e.g. for a SBO

As described in section 6.1.2.1, PDHR [JN02] variants 1, 2, and 4 place requirements onto the HPIS [JND], however will use the LVCS [KBA] for inventory control if available. PDHR [JN02] variant 3 places requirements onto the LPIS [JNG] for a small set of faults (SBO), which is also required to support ECC [JN01] operation; the ALARP aspects are described in section 6.1.2.10.3.

Active inventory control in the steam and feed systems (secondary) is not required during PDHR [JN02] cooling because the cooling circuit between the SGs and the PSCS [JNB] is closed loop. Inventory control in the LUHS [JNK] (tertiary) is generally not required during PDHR [JN02] operation because they are sized to meet the long-term (72 hour) heat removal requirements without active inventory control. In the infrequent scenario where only a single PSCS [JNB] train is successfully aligned for heat removal, then it is necessary to open a valve on the cross connect lines between two LUHS [JNK] tertiary tanks to extend cooling from 24 hours to 72 hours.

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.

As described in section 6.1.2.1, PDHR [JN02] variants 1, 2, and 4 place requirements onto the HPIS [JND], however will use the pressuriser heaters for pressure control if available. PDHR [JN02] variant 3 places requirements onto the LPIS [JNG] gas bubble for a small set of faults (SBO), which is also required to support ECC [JN01] operation; the ALARP aspects are described in section 6.1.2.10.3.

The secondary pressure will typically be a function of the RCS [JE] temperature, therefore as RCS [JE] temperature falls throughout PDHR [JN02] operation the steam pressure will fall correspondingly. In some fault sequences e.g. SBO, PSCS [JNB] cooling will not initiate in the early phases of these faults because SG low level is not reached, resulting in high pressure. If high pressure is detected in these scenarios in the steam system, the ASD [LBK50] valves open and discharge steam to the atmosphere until the desired steam pressure is attained, at which point the valves close.

Should ASD [LBK50] fail to initiate, PDHR [JN02] would continue to operate successfully with secondary over-pressure protection provided by the passive SG Relief System [LBK10] (although PDHR [JN02] does not place a deterministic E3S requirements on this system).

For SB and isolable IB LOCAs, PDHR [JN02] will isolate the leak by automatically commanding the CVCS [KB] and Nuclear Sampling System [KUA] isolation valves shut upon low pressuriser level.

The key performance and design parameters for PDHR [JN02] are presented in Table 6.1-7. Simplified schematics of the key SSC contributing to PDHR [JN02] operation are illustrated in Figure 6.1-2, Figure 6.1-3 and Figure 6.1-4.

Table 6.1-7: Key Design and Performance Parameters for PDHR [JN02]

Parameter	Value
Maximum RCS [JE] operating pressure	{REDACTED}
Minimum RCS [JE] operating pressure (after 72 hrs cooling)	{REDACTED}
Maximum RCS [JE] temperature (hot leg)	{REDACTED}
Minimum RCS [JE] temperature (cold leg, after 72 hrs cooling)	{REDACTED}
RCS [JE] loop redundancy	1oo3
Maximum HPIS [JND] Flow Rate (at RCS [JE] normal operating pressure	{REDACTED}
HPIS [JND] injection pump redundancy	1oo2
Maximum steam pressure	{REDACTED}
Minimum steam pressure (after 72 hrs cooling)	{REDACTED}
Maximum steam temperature	{REDACTED}
Minimum steam temperature (after 72 hrs cooling)	{REDACTED}
PSCS [JNB] heat exchanger maximum thermal duty	{REDACTED} ({REDACTED} per train)
PSCS heat exchanger redundancy	1oo3

Parameter	Value
ASD [LBK50] redundancy	1oo2 (per SG)
Maximum LUHS [JNK] operating temperature	{REDACTED}
Maximum LUHS [JNK] operating pressure	{REDACTED}
LUHS boil-off inventory	{REDACTED} (per train)
LUHS redundancy	1oo3 (24 hrs) 2oo3 (72 hrs)

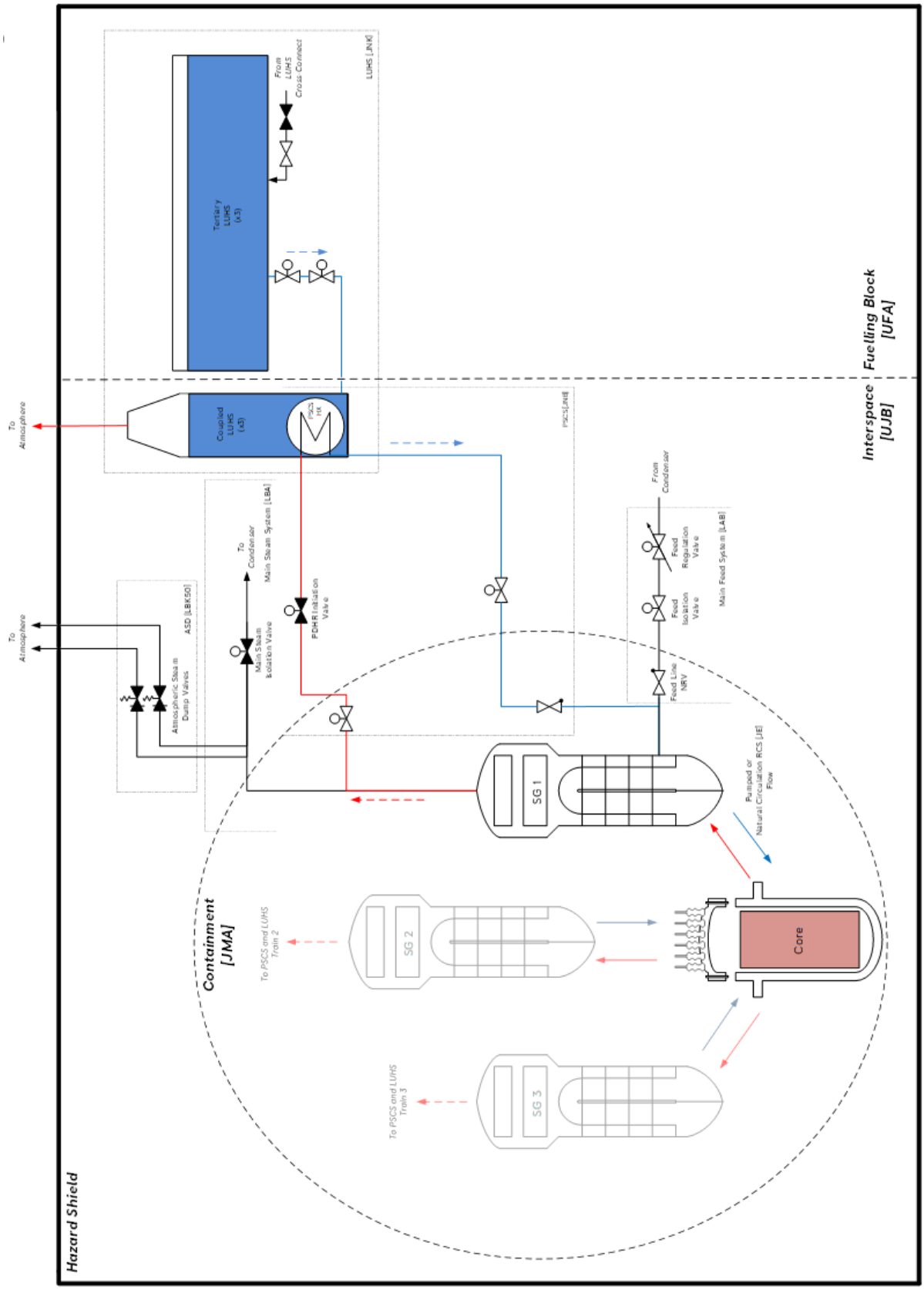


Figure 6.1-2: Simplified Schematic of PDHR [JN02] (Heat Removal)

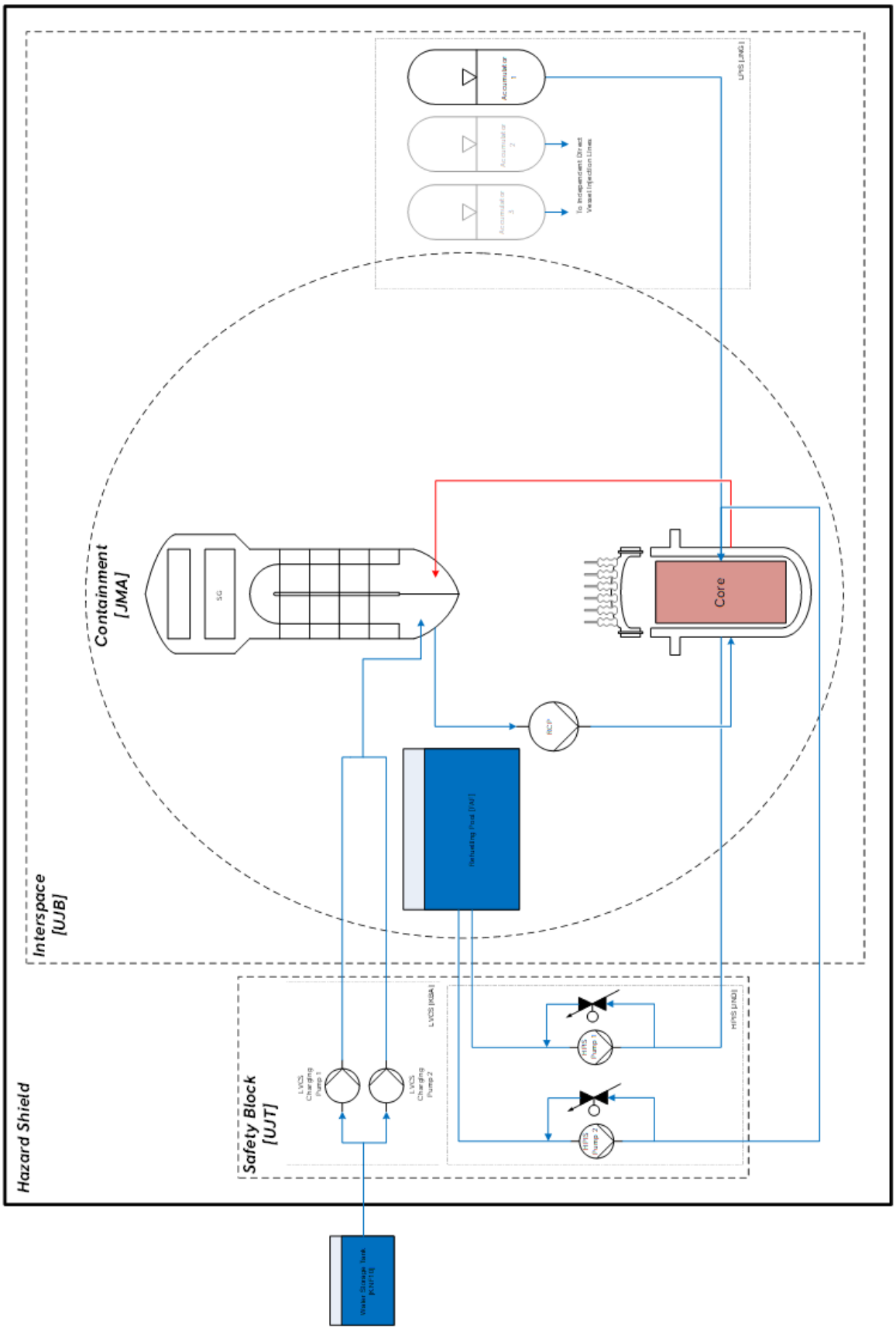


Figure 6.1-3: Simplified Schematic of PDHR [JN02] (Inventory Control)

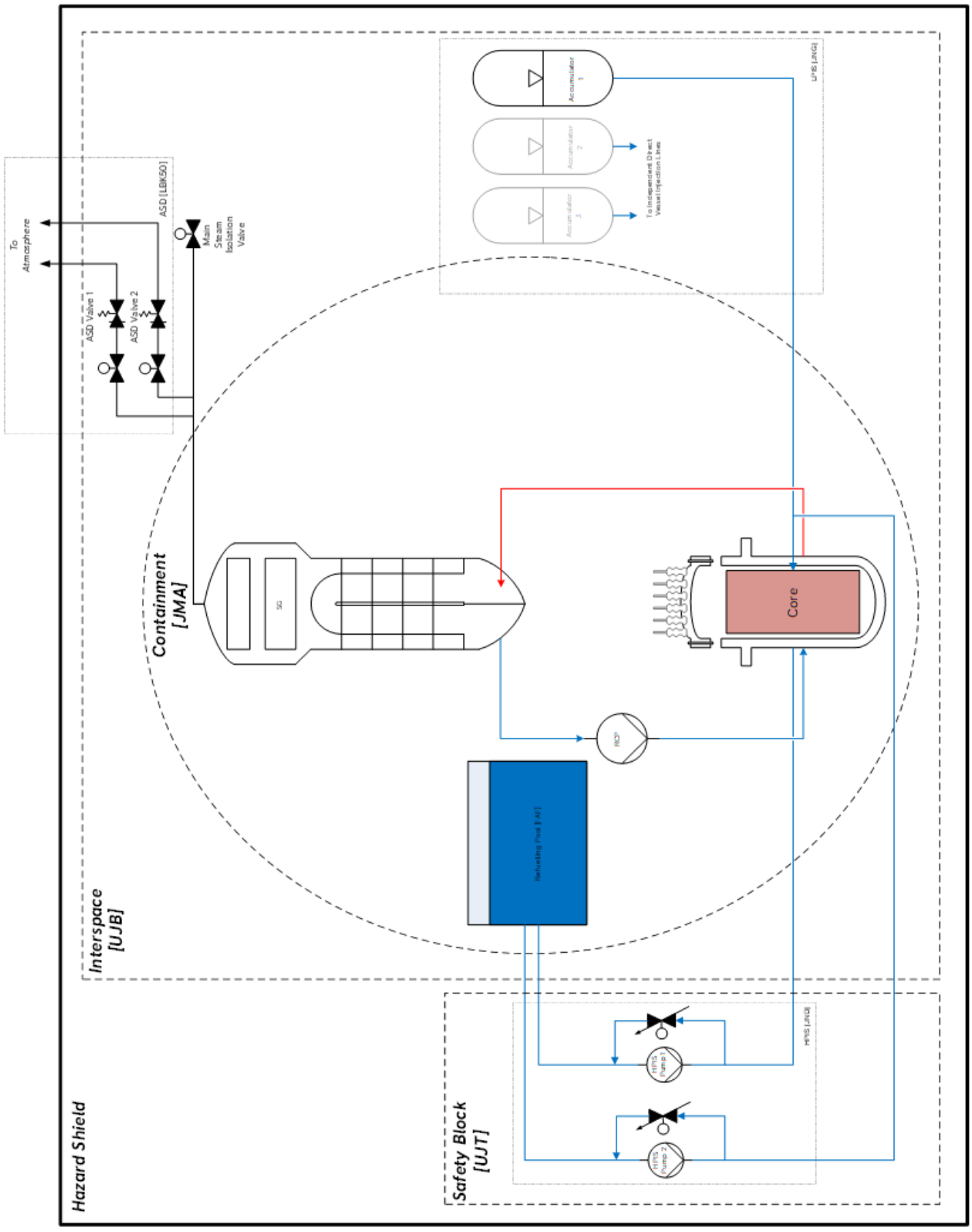


Figure 6.1-4: Simplified Schematic of PDHR [JN02] (Pressure Control)

The PDHR [JN02] allocates E3S requirements to a range of SSCs that deliver its functions, described further in [9], including:

- PSCS [JNB]
- LUHS [JNK]
- HPIS [JND]
- LPIS [JNG]
- Steam Generation System [JEA]
- Main Steam System [LBA] (specifically the piping and MSIVs on Reactor Island [LBA20])
- Main Feedwater System [LAB] (specifically the piping and feedwater isolation valves on Reactor Island [LAB20])
- ASD [LBK50]
- SG Purification System [LCQ]
- Reactor System [JA]
- RCS [JE]
- Reactor Coolant Pressurising System [JEF]
- CVCS [KB]
- Nuclear Sampling System [KUA]
- RPS2 [JRA20].

It is noted that the Main Steam System [LBA] and the Main Feedwater System [LAB] span across both Reactor Island and Turbine Island. The PDHR [JN02] places safety category B functions onto the Reactor Island parts of the system.

The developing layout of the key SSC supporting PDHR [JN02] operation is summarised in [11]. Each of the key sub-systems delivering the PDHR [JN02] are located within the hazard shield and on the aseismic bearing to provide protection against external hazards.

Separation and segregation of redundant trains is adopted within the layout to ensure the PDHR [JN02] can deliver its function in the event of an internal hazard, examples include:

- The LUHS [JNK] tanks are spatially segregated and contained within the buttresses of the Interspace [UJB] in the northeast, northwest, and southeast corners
- The two HPIS [JND] trains are entirely segregated by a partition wall, within the Safety Systems Block [UJT]

Further description of the PDHR [JN02] safety measure, including detail of the associated sub-systems and components, is provided in the PDHR SMDD [19].

6.1.2.4 Materials

The description and justification of materials used for Class 2 SSCs are presented in E3S Case Chapter 23: Structural Integrity [1].

6.1.2.5 Interfaces with Supporting Systems

The PDHR [JN02] is designed to operate in conjunction with either Scram [JD01] or Alternative Shutdown Function (ASF) [JD02] for CoR, except for PDHR [JN02] variant 3 which is required for infrequent faults and therefore not compatible with ASF [JD02].

The PDHR [JN02] is automatically initiated by the C&I system, specifically the RPS2 [JRA20] within the Reactor Control and Protection System [JY], see section 6.1.2.7.

The PDHR [JN02] components that require power are supplied from the grid or Main Generator [MK] (house load operation). During a LOOP, power to the PDHR [JN02] components is supplied from the standby AC power supplies in the High Voltage Power Generation System [BDV], with the Low Voltage Uninterruptible DC Supply System for Safety Services [BQ] providing power (from batteries) for any C&I and actuation that is required during the start-up of the standby AC power. During a SBO, the Uninterruptible AC Supply System [BM] and the Low Voltage Uninterruptible DC Supply System for Safety Services [BQ] provide power (from batteries) for the required C&I and valve actuation. The electrical power systems are described further in E3S Case Chapter 8: Electrical Power System [12].

6.1.2.6 System and Equipment Operation

6.1.2.6.1 Normal Operation

The Reactor Island Operating Philosophy [13] 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 [14].

During operating mode 1 (power operation), the PDHR [JN02] is maintained in a standby state. 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 operating mode 1. During operating modes 3 (hot standby) and 4a (hot shutdown – steaming), 4b (hot shutdown – non-steaming), the PDHR [JN02] will be available in standby and configured as per operating mode 1. The PDHR [JN02] is not required for all remaining operating modes, therefore components that are not required for other protective safety measures will be made available for EMIT activities.

The component configuration for PDHR [JN02] in standby during all normal operating modes are listed in [19].

6.1.2.6.2 Operation during Faults

Following all PIEs, the reactor will be shutdown through either Scram [JD01] or the ASF [JD02]. Decay heat removal after reactor shutdown will be provided by HTHR [JN03] when a heat removal path from the SGs to the condenser or ASD [LBK50] is available. If the condenser is unavailable, then decay heat removal can be provided for several hours via SG bleed and feed, where the main feed or auxiliary feed pumps supply feedwater to the SGs and the ASD [LBK50] provides a bleed path to

the environment. If all feed is unavailable, then PDHR [JN02] is the first CoFT protective safety measure.

PDHR [JN02] is automatically initiated upon detection of low level in two of the three SGs (it 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.

The RPS2 [JRA20] then controls the HPIS [JND] injection pump spillback to ensure pressure does not fall below the margin to saturation in the cold leg (to provide margin to ECC [JN01] initiation on saturation) and does not exceed a pressure that would result in a reactor pressure relief valve lift. In the event both CVCS [KB] and HPIS [JNB] are unavailable, LPIS [JND] is initiated automatically when the pressure falls below {REDACTED}.

Specific operating responses to a range of fault conditions are presented in the PDHR SMDD [19].

6.1.2.7 Instrumentation & Control

All PDHR [JN02] functionality can be automatically initiated without reliance on the operator for at least 72 hours following all PIEs. This is achieved through a series of automatic control and instrumentation functions, described in [19].

PDHR [JN02] places several trip functions onto the Reactor Control and Protection System [JY] for initiation. The Reactor Control and Protection 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 SCR. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits.

The Reactor Control and Protection System [JY] and allocation of safety categorised functional requirements from the PDHR [JN02] is described further in E3S Case Version 2, Tier 1, Chapter 7: Instrumentation & Control [15].

6.1.2.8 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.

The EMIT activities for the PDHR [JN02] are defined as TLA within the RR SMR requirements management database, and cover safety derived tasks (ISI, reliability derived tasks (RCM/preventative maintenance), and industry best practice/OPEX (EPRI PMBD).

6.1.2.9 Radiological Aspects

PDHR [JN02] is required in response to 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. Radiological consequences for fault sequences are described further in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.1.2.10 Performance and Safety Evaluation

6.1.2.10.1 Compliance with Safety Categorised Functional Requirements

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 primarily include performance analysis using RELAP5-3D and VIPRE-01 codes, with integrated effects testing to validate analysis.

Performance analysis demonstrates that the PDHR [JN02] successfully removes heat to deliver its safety function for all fault conditions at RD7/DRP1. The output of performance analysis and margin to acceptance criteria for the PDHR [JN02] are presented in [19], with the suite of performance analysis for bounding fault conditions that place safety categorised functional requirements on the PDHR [JN02] presented in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.1.2.10.2 Compliance with Non-Functional System Requirements

A summary of the compliance for non-functional system requirements allocated to the PDHR [JN02] are summarised in Table 6.1-8. Further details are provided in [16] and [19].

Table 6.1-8: PDHR [JN02] Non-Functional System Requirements Compliance

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN02-R-2111	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.	PDHR [JN02] is designed with three redundant coolant trains which are segregated such that a single internal hazard in unlikely to result in CCF of more than one train of PDHR [JN02].
JN02-R-2112	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.	All SSCs which support PDHR [JN02] are contained within and supported upon the Hazard Shield and Aseismic Bearing respectively. PDHR [JN02] is designed with redundant trains which are segregated such that a single external hazard in unlikely to result in CCF of more than one train PDHR [JN02].
JN02-R-2119	Safety measures shall deliver the defined success criteria.	Performance analysis demonstrates that the PDHR [JN02] successfully removes heat to deliver its safety function.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN02-R-1997	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.	PDHR [JN02] is designed with suitable redundancy in line with RGP and OPEX to ensure resilience to random faults. The redundancy requirements allocated to all sub-systems and components which support the safety measure are summarised in Table 6.1-7. PDHR [JN02] is functionally diverse to the ECC [JN01] CoFT safety measure.
JN02-R-1996	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.	PDHR [JN02] is designed to deliver its functions in response to the most onerous initial operating states. Performance analysis which supports safety measure design uses a combined approach including a best-estimate analysis method with conservative assumptions, including initial and boundary conditions.
JN02-R-1978	The design shall fail to a safe state where practicable	Valves that move position in response to a safety demand from the C&I systems or are in pipework that supports successful PDHR [JN02] operation, are specified to fail to a safe position upon loss of power. RCPs include flywheels, which provide an elongated coast-down following a loss of primary flow fault. Sensors fail to a trip state, which places the associated RPS/DPS logic train into a tripped state.
JN02-R-2009	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.	For each bounding design basis fault, the PDHR [JN02] ensures selected trip parameters relate directly to the fault, where practicable, in order to provide rapid response.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JN02-R-2003	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.	For all design basis fault conditions, the PDHR [JN02] safety measure initiates automatically without operator action.
JN02-R-2004	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.	The design of the PDHR [JN02] ensures no essential services are needed from on-site mobile equipment for 72 hours. After a prolonged period of PDHR [JN02] operation (>72 hours), the LUHS [JNK] level could fall to such an extent that further water is required to continue reactor cooling. Long-term cooling for the PDHR [JN02] solutions is being designed to ensure no essential services are needed from off-site for 7 days.
JN02-R-2011	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.	The PDHR [JN02] is designed to interface with offsite equipment in deliver of its categorised functions, primarily via external top up lines to the LUHS [JNK].
JN02-R-2572	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.	Human factors assessment ensure integration through the design process, including human factors checklists, allocation of function, task analysis and human reliability analysis.

6.1.2.10.3 ALARP, BAT, Secure by Design and Safeguards by Design

Key PDHR [JN02] design decisions made with respect to ensuring overall risks are reduced to ALARP, BAT, secure by design and safeguards by design include:

- Design to ensure significant functional diversity to the ECC [JN01] that provides the second CoFT protective safety measure. Components that are shared justified based on RGP and overall risk reduction:
    - The LUHS tanks already comprise redundancy of large passive water stores and the safety risk reduction of further redundancy is minimal. There are also diverse

heatsinks to the LUHS [JNK] for the reactor plant, e.g. cooling towers. Additional water sources would significantly increase the footprint of the plant and the hazard shield

- A single MSIV on each steam line to provide isolation is based on RGP, with further valve diversity being explored such as diverse actuation

- The Refuelling Pool [FAF] that provides water for the HPIS [JND] and the ECC [JN01] gravity drain is a massive and passive structure with high reliability claims on its structural integrity, and the CoFT safety function can be delivered for both leaks and structural failure

- 1oo3 redundancy for the PDHR cooling trains and heat exchangers provide improved reliability over 2oo3 options for Class 2 systems

- Improved defence in depth provisions of pressure and inventory control by both active and passive means.

More detailed information on design decisions is presented in the PDHR SMDD [19] and associated design decision files.

6.1.3 High Temperature Heat Removal

6.1.3.1 System and Equipment Functions

The function of the HTHR [JN03] is to remove residual heat from the reactor core via the condenser or ASD to the atmosphere. The HTHR [JN03] preventive safety measure facilitates delivery of the FSF of CoFT.

6.1.3.2 Design Basis

The HTHR [JN03] provides a safety category C function of decay heat removal following PIEs that occur in operating modes 1 through to 4a, to provide the preventive line of defence in depth.

E3S functional and non-functional system requirements for HTHR [JN03] will be reported in Version 3 of the generic E3S Case.

6.1.3.3 Description

The HTHR [JN03] uses the SGs and the normal duty steam condenser or ASD [LBK50] to cool the primary plant. Heated primary coolant is pumped via the RCPs to the SGs where heat is transferred though the SG tube walls to lower pressure secondary coolant. The secondary coolant boils to generate pressurised steam that is transferred to the condenser to ultimately transfer heat to the atmosphere, with condensed coolant circulated back to the SG. If the condenser is unavailable, the pressurised steam can be transferred to the ASD [LBK50] and released to the atmosphere.

The design of the HTHR [JN03] and the detailed description of the safety measure will be reported in Version 3 of the generic E3S Case.

6.1.4 Low Temperature Decay Heat Removal

6.1.4.1 System and Equipment Functions

The function of the Low Temperature Decay Heat Removal (LTDHR) [JN04] safety measure is to remove residual heat from the reactor core during faulted shutdown and refuelling operations. The LTDHR [JN04] safety measure provides the FSF of CoFT in response to frequent faults.

6.1.4.2 Design Basis

The LTDHR [JN04] safety measure provides a safety category B function of decay heat removal for faulted plant shutdown during operating modes 4b through to 6b. It provides the first protective line of defence in depth during DBC-3i frequent faults.

E3S functional and non-functional system requirements for the LTDHR [JN04] will be reported in Version 3 of the generic E3S Case.

6.1.4.3 Description

The LTDHR [JN04] uses the CSCS [JNA], Component Cooling System (CCS) [KAA] and Essential Service Water System (ESWS) cooling towers [PBD] as the cooling chain for removal of heat from the RPV [JAA] to atmosphere.

The design of the LTDHR [JN04] and the detailed description of the safety measure will be reported in Version 3 of the generic E3S Case

6.2 Emergency Reactivity Control Systems

6.2.1 Scram

6.2.1.1 System and Equipment Functions

The function of Scram [JD01] is to provide the principle means of achieving the FSF of CoR during faulted operation by inserting negative reactivity in the form of solid neutron absorbers into the reactor fuel, thereby shutting down the reactor and providing shutdown margin (SDM) to cold zero power (CZP).

6.2.1.2 Design Basis

6.2.1.2.1 Functional Requirements

Safety categorised functional requirements for Scram [JD01] based on the HLSFs they deliver are presented in Table 6.2-1 based on [20].

Table 6.2-1: Scram [JD01] Safety Categorised Functional Requirements

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JD01-R-1271	When relevant faults occur, Scram [JD01] (DBC-2ii and DBC-3i) shall shutdown the reactor through negative reactivity insertion.	1, 2	A
JD01-R-2432	When relevant faults occur, Scram [JD01] (DBC-3ii and DBC-4) shall shutdown the reactor through negative reactivity insertion.	1, 2	A

Scram [JD01] provides the principal means of CoR for frequent and infrequent faults and therefore the functions it performs are safety category A. The relevant PIEs that Scram [JD01] is claimed against are listed in [20].

The safety categorised functional requirements for Scram [JD01] are flowed down and allocated to relevant sub-systems and/or components in [21]. Non-functional performance requirements associated with the safety categorised functional requirements are allocated in [20].

6.2.1.2.2 Non-Functional System Requirements

Non-functional system requirements are allocated to Scram [JD01] based on the E3S design principles as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2], summarised in Table 6.2-2.

Table 6.2-2: Scram [JD01] Non-Functional System Requirements

Requirement ID	Non-Functional System Requirement
JD01-R-2627	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.
JD01-R-2628	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.
JD01-R-2629	Safety measures shall deliver the defined success criteria.
JD01-R-2632	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the presence of a single failure.
JD01-R-2613	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the worst normally permitted configuration of equipment outages for maintenance, test, or repair.
JD01-R-2540	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
JD01-R-2539	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.
JD01-R-2533	The design shall fail to a safe state where practicable
JD01-R-2614	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions with diverse means of initiation to the extent reasonably practicable, which shall be via the use of different variables, when the measure requires automatic initiation.
JD01-R-2548	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.
JD01-R-2547	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.
JD01-R-2550	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.

Requirement ID	Non-Functional System Requirement
JD01-R-2551	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.
JD01-R-2558	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.

6.2.1.2.3 E3S Classification

Safety Classification

Scram [JD01] is the principal means by which the safety category A function is achieved, and in accordance with the E3S categorisation and classification methodology outlined in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives & Design Rules [2], the minimum safety classification of components within the system is safety class 1.

Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

Seismic Performance Classification

The seismic performance classification will principally be SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.2.1.3 Description

A soluble boron-free chemistry regime for duty reactivity control and Scram [JD01] has been developed for the RR SMR, meaning that full SDM can be achieved by the control rods without the addition of boron (a diverse means of shutting down the reactor through boron injection is provided by the ASF [JD02], described in section 6.2.2).

Scram [JD01] relies on successful insertion of the control rods with associated Control Rod Drive Mechanisms (CRDMs). It is also reliant on instrumentation predominantly within the RCS [JE] and response of the Reactor Control and Protection Systems [JY].

During powered operations, the control rods are vertically positioned by the CRDMs, by way of a drive rod which connects the two. The CRDM actuators are positioned on the top of the RPV Head [JAB] and their pressure boundary extends at sufficient height to allow the drive rod and control rods to be fully withdrawn from the Fuel Assemblies [JAK]. The RPV internals ensure alignment of the control rods within the RPV [JAA]. The CRDMs, Fuel Assemblies [JAK] and RPV internals sit within the Reactor Core System [JAC], which in turn sits within the Reactor System [JA].

Scram [JD01] is demanded when relevant trip conditions are detected by instrumentation in duty systems or through manual initiation by the operator. In response to this demand, the Reactor Control and Protection Systems [JY] open reactor trip breakers to cut power to the CRDMs which release the control rods (loss of electrical supply to the CRDMs also release the control rods). The control rods fall under gravity and are guided by the RPV internals into the Fuel Assemblies [JAK] to provide complete SDM.

The baseline key performance and design parameters for Scram [JD01] are presented in Table 6.2-3. A simplified schematic is illustrated in Figure 6.2-1.

Table 6.2-3: Key Design and Performance Parameters for Scram [JD01]

Parameter	Value
Total number of control rods	89 (within 121 Fuel Assemblies [JAK])
Required time for control rods to reach bottom of core (from trip setpoint reached)	3.9 s
Number of control rods (N) required for shutdown to Cold Zero Power	88 (N-1)

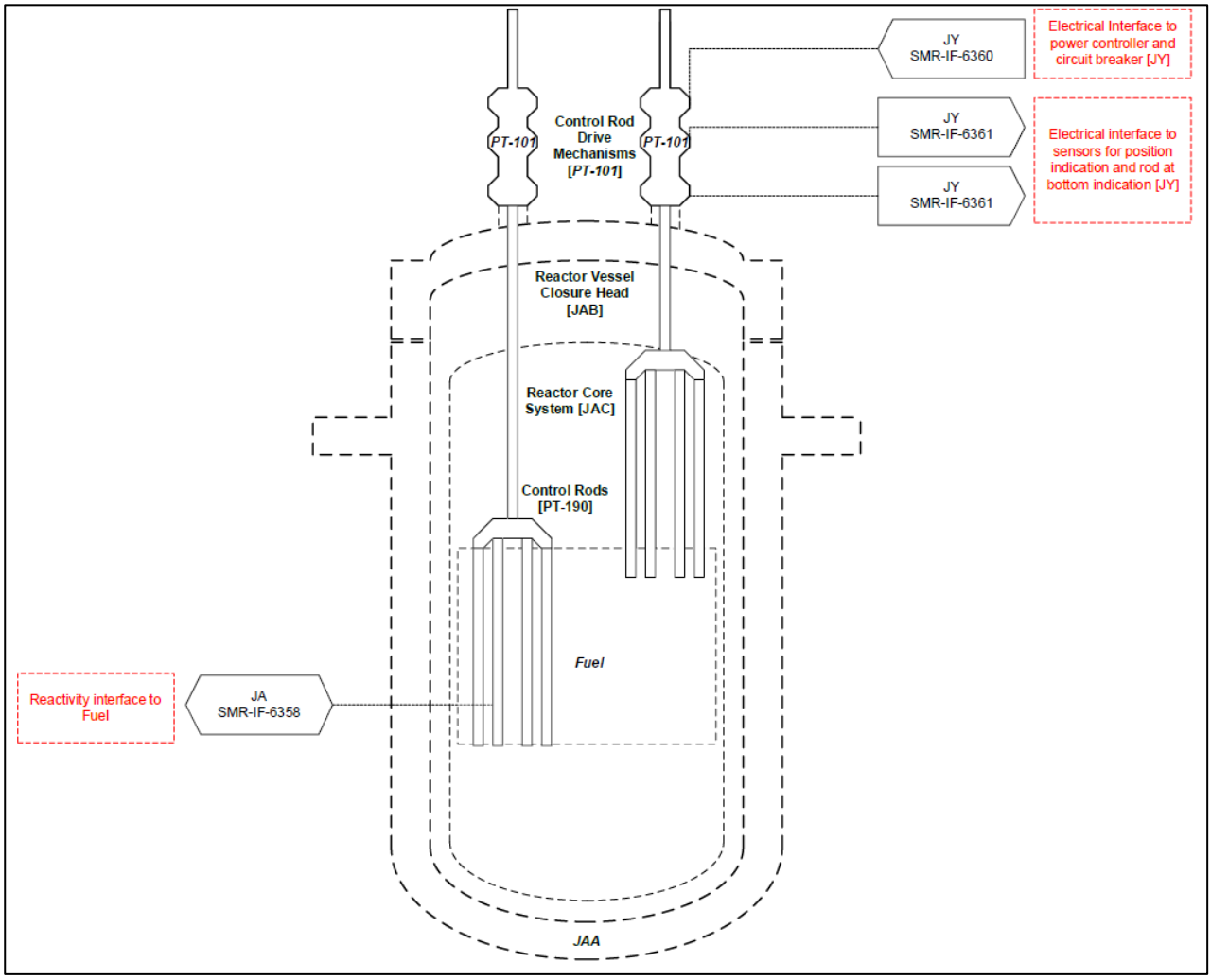


Figure 6.2-1: Scram [JD01] Schematic

The developing layout of SSC supporting Scram [JD01] operation is summarised in [11]. Each of the key sub-systems delivering Scram [JD01] are located within the hazard shield and on the aseismic bearing to provide protection against external hazards.

Further description of Scram [JD01], including detail of the associated sub-systems and components, is provided in the Scram SMDD [22].

6.2.1.4 Materials

The description and justification of materials used for safety class 1 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.2.1.5 Interfaces with Supporting Systems

Scram [JD01] interfaces with safety measures providing the FSF of CoFT, which need to function together successfully to provide full protection of the core.

Scram [JD01] is designed to operate prior to and alongside HTHR [JN03] preventative safety measures (section 6.1.3), as well as PDHR [JN02] (section 6.1.2) and ECC [JN01] (section 6.1.1) protective safety measures. Scram [JD01] and PDHR [JN02] (first line of protective safety) are also designed to ensure they do not initiate the second line of protective safety, ASF [JD02] and ECC [JN01] respectively, when operating successfully.

Scram [JD01] is reliant on systems and sub-systems to ensure the control rods are rapidly inserted into the core in response to faulted conditions. Key supporting systems include the Reactor System [JA], Reactor Core System [JAC], Reactor Control and Protection Systems [JY], and the RCS [JE].

In the event of loss of power supply to the instrumentation supporting Scram [JD01], a trip signal will be sent to the reactor trip breakers. In the event of any loss of power supply to the CRDMs, the control rods will be released, and the control rods will drop into the core. It is noted that following a loss of external grid from 100 % power, Scram [JD01] does not initiate following a trip to house load in accordance with RGP from the EURs.

6.2.1.6 System and Equipment Operation

6.2.1.6.1 Normal Operation

The Reactor Island Operating Philosophy [13] 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 Version 2, Tier 1, Chapter 13: Conduct of Operations [14].

During Operating Mode 1 (power operation), Scram [JD01] will be on standby, the CRDMs will be powered, engaged and will either be holding the control rods 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. Scram [JD01] will only initiate in the event of instrumentation trip values being reached or if manually activated in the MCR.

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

During Operating Mode 3 (Hot Standby), Scram [JD01] is not required as the control rods 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 rod control gear power 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 CRDMs will be removed to access in the RPV [JAA] internals. Reactivity control and hold down must be maintained by the fuel handling system as Scram [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.

6.2.1.6.2 Operation during Faults

The primary function of Scram [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 power supply), the RPS [JRA] or the DPS [JQA] will provide commands to interrupt the power supplies to the CRDMs that are holding the control rods 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 to CZP. Manual initiation is also possible from the MCR.

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, {REDACTED}.

To provide diversity of automatic initiation, Scram [JD01] requires definition of one RPS [JRA] trip and one DPS [JQA] trip for each fault. Either of these trips needs to be capable of independently initiating Scram [JD01] (see section 6.2.1.7)

Specific operational responses to fault conditions are described in [22].

6.2.1.7 Instrumentation & Control

Scram [JD01] is deterministically designed so that no reliance is placed on the operator following initiation of all DBC faults, noting manual initiation of Scram [JD01] from the MCR is possible.

Scram [JD01] places several trip functions onto the RPS [JRA] and DPS [JQA] within the Reactor Control and Protection System [JY], which will also monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the SCR.

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 SMDD [22]. The allocation of safety categorised functional requirements from Scram [JD01] to the Reactor Control and Protection System [JY] is presented in the C&I Engineering Schedule, described further in E3S Case Version 2, Tier 1, Chapter 7: Instrumentation & Control [15], with further details provided in Scram SMDD [22].

6.2.1.8 Monitoring, Inspection, Testing and Maintenance

The design life of the RR SMR is intended to be 60 years, though some components of Scram [JD01] will need to be replaced within that period.

The EMIT activities for Scram [JD01] are defined as TLA within the RR SMR requirements management database, and cover safety derived tasks (ISI, reliability derived tasks (RCM/preventative maintenance), and industry best practice/OPEX (EPRI PMBD).

6.2.1.9 Radiological Aspects

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

6.2.1.10 Performance and Safety Evaluation

6.2.1.10.1 Compliance with Safety Categorised Functional Requirements

Verification strategies for Scram [JD01] and associated sub-systems to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements primarily include performance analysis using RELAP5-3D and VIPRE-01 codes, with core flow and boron mixing rig testing to validate analysis, and a CRDM verification strategy from the vendor.

Performance analysis demonstrates that Scram [JD01] can be successfully initiated within required timescales to deliver its safety function for all fault conditions at RD7/DRP1. The output of performance analysis and margin to acceptance criteria for Scram [JD01] are presented in [22], with the suite of performance analysis for bounding fault conditions that place safety categorised functional requirements on Scram [JD01] presented in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.2.1.10.2 Compliance with Non-Functional System Requirements

A summary of the compliance for non-functional system requirements allocated to Scram [JD01] are summarised in Table 6.2-4. Further details are provided in [20] and [22].

Table 6.2-4: Scram [JD01] Non-Functional System Requirements Compliance

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD01-R-2627	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.	The trains of the C&I RPS [JRA] and DPS [JQA] are separated and segregated to provide protection to internal hazards.
JD01-R-2628	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.	All Class 1 SSCs which support Scram [JD01] are contained within and supported upon the Hazard Shield and Aseismic Bearing respectively.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD01-R-2629	Safety measures shall deliver the defined success criteria.	Performance analysis demonstrates that Scram [JD01] successfully removes heat to deliver its safety function
JD01-R-2632	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the presence of a single failure.	Scram [JD01] is designed with redundancy to be tolerant to a single failure, including failure of instrumentation, protection systems, Scram breakers and CRDMs.
JD01-R-2613	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the worst normally permitted configuration of equipment outages for maintenance, test, or repair.	The multiple CRDMs and control rods will not have any planned EMIT during normal operation.
JD01-R-2540	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.	Scram [JD01] is designed with redundancy to be tolerant to a single failure, including failure of instrumentation, protection systems, Scram breakers and CRDMs. Scram [JD01] is functionally diverse to the ASF [JD02] CoR safety measure; each safety measure relies on different physical phenomena to insert negative reactivity into the core.
JD01-R-2539	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.	ECC [JN01] is designed to deliver its functions in response to the most onerous initial operating states. Performance analysis which supports safety measure design use a combined approach including a best-estimate analysis method with conservative assumptions, including initial and boundary conditions.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD01-R-2533	The design shall fail to a safe state where practicable	Failure of electrical supplies to the CRDMs will result in the control rods dropping into the core, initiating Scram [JD01]. Reactor trip breakers will fail to an open state, initiating Scram [JD01]. The RCPs include flywheels, which provide an elongated coast-down following a loss of primary flow fault. The coast down period ensures that sufficient cooling flow is maintained through the reactor to maintain the core within specified limits to support Scram [JD01] operation.
JD01-R-2614	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions with diverse means of initiation to the extent reasonably practicable, which shall be via the use of different variables, when the measure requires automatic initiation.	Diverse means of automatic initiation are provided in the RPS [JRA] and DPS [JQA].
JD01-R-2548	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.	For each DBC (DBC-2ii/3i/3ii/4), Scram [JD01] has two diverse trips off different instrumentation and variables.
JD01-R-2547	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.	For each DBC (DBC-2ii/3i/3ii/4), Scram [JD01] initiates automatically without operator action. Once rods have passively been inserted into the core, no further operator action is required.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD01-R-2550	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.	For each DBC (DBC-2ii/3i/3ii/4), Scram [JD01] initiates automatically without operator action. Once rods have passively been inserted into the core, scram needs no further operator action or essential services.
JD01-R-2551	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.	Scram [JD01] passively initiates upon failure of electrical supplies. The safety measure doesn't require other services to fulfil its function. Following Scram initiation, no further services are required to maintain SDM.
JD01-R-2558	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.	Human factors assessment ensure integration through the design process, including human factors checklists, allocation of function, task analysis and human reliability analysis.

6.2.1.10.3 ALARP, BAT, Secure by Design and Safeguards by Design

Key Scram [JD01] design decisions made with respect to ensuring overall risks are reduced to ALARP, BAT, secure by design and safeguards by design include:

- 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 safety 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 SMDD [22] and associated design decision files.

6.2.2 Alternative Shutdown Function

6.2.2.1.1 System and Equipment Functions

The function of ASF [JD02] is to provide the diverse means of achieving the FSF of CoR during faulted operation by the injection of soluble boron (potassium tetraborate) into the reactor, which acts as a soluble neutron absorber to ensure adequate SDM above a certain concentration, holding the plant in a sub-critical condition.

ASF [JD02] has two ‘variants’ of the safety measure within the fault schedule at RD7/DRP1, including:

- ASF [JD02] variant 1 – automatic initiation
- ASF [JD02] variant 2 – manual initiation

6.2.2.2 Design Basis

6.2.2.2.1 Functional Requirements

Safety categorised functional requirements for ASF [JD02] based on the HLSFs they deliver are presented in Table 6.2-5 based on [23].

Table 6.2-5: ASF [JD02] Safety Categorised Functional Requirements

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JD02-R-1273	When relevant faults occur, ASF [JD02] Variant 1 (Automatic Initiation) shall shutdown the reactor through negative reactivity insertion via the injection of soluble Boron (potassium tetraborate).	1, 2	B

ASF [JD02] provides the diverse means of shut and hold down of the reactor for DBC-4 frequent faults with failure of the first measure, and therefore the functions performed are safety category B. The relevant PIEs that ASF [JD02] is claimed against are listed in [23].

The safety categorised functional requirements for ASF [JD02] are flowed down and allocated to relevant sub-systems and/or components in [24]. Non-functional performance requirements associated with the safety categorised functional requirements are allocated in [23].

No environment, security or safeguards functional requirements are assigned at RD7/DRP1.

6.2.2.2.2 Non-Functional System Requirements

Non-functional system requirements are allocated to ASF [JD02] based on the E3S design principles as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2], summarised in Table 6.2-6.

Table 6.2-6: ASF [JD02] Non-Functional System Requirements

Requirement ID	Non-Functional System Requirement
JD02-R-1709	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.
JD02-R-1710	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.
JD02-R-1711	Safety measures shall deliver the defined success criteria.

Requirement ID	Non-Functional System Requirement
JD02-R-1692	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
JD02-R-1694	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.
JD02-R-1695	The design shall fail to a safe state where practicable
JD02-R-1697	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.
JD02-R-1699	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.
JD02-R-1700	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.
JD02-R-1701	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.
JD02-R-1702	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.

6.2.2.2.3 E3S Classification

Safety Classification

ASF [JD02] provides a safety category B function and in accordance with the E3S categorisation and classification methodology outlined in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2], the safety classification of components within the system is safety class 2. It is noted that some components, including the containment isolation valves, also provide support to the ECC [JN01] (see section 6.1.1) and therefore are safety class 1.

Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

Seismic Performance Classification

The seismic performance classification will principally be SPC1 in accordance with E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.2.2.3 Description

The baseline architecture for ASF [JD02] comprises of the Emergency Boron Injection System (EBIS) [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]. ASF [JD02] also utilises instrumentation predominantly within the RCS [JE] and response of the Reactor Control and Protection Systems [JY].

The functional operation is split into two phases:

1. Enriched boron-10 potassium tetraborate solution is delivered from a boron storage tank to the DVI nozzles of the RPV [JAA] with a quantity sufficient to borate the entire RCS [JE]. This solution is also delivered to and mixed with the Refuelling Pool [FAF] to support phase 2 operation.

2. Pre-mixed potassium tetraborate solution is delivered from the Refuelling pool [FAF] to the DVI nozzles of the RPV [JAA].

The EBIS [JDK] stores concentrated potassium tetraborate solution in a boron storage tank, isolated from the plant during normal operation. Two independent trains from the boron storage tank supply the HPIS [JND] when demanded, which ultimately directs boron into the RPV [JAA]. This part of the EBIS [JDK] system operates at low pressure and is dependent on the HPIS [JND] injection pumps.

The EBIS [JDK] boron storage tank also supplies two independent EBIS [JDK] trains that route to the Refuelling Pool [FAF], with each train comprising of a pump, valves, pipework and instrumentation to supply a sufficient quantity of potassium tetraborate solution to the Refuelling Pool [FAF]. The EBIS [JDK] pumps are used to mix the Refuelling Pool [FAF] to ensure a consistent concentration throughout the pool, ready to be used in ASF [JD02] phase 2.

The HPIS [JDK] provides the driving head needed to overcome the RPV [JAA] operating pressure and deliver potassium tetraborate for shutdown, from either the EBIS [JDK] system or coolant / borated coolant from the Refuelling Pool [FAF] to the DVI nozzles.

The recirculation trains are used to take coolant / borated coolant that has exited the RCS [JE] in a LOCA scenario, condensed and collected in the containment sump, and return it to the Refuelling Pool [FAF], to ensure that there is sufficient inventory to be injected over the required mission time.

It is noted for ICFs or LOCAs with successful Scram [JD01], HPIS [JND] is required to operate to support PDHR [JN02] only to make up inventory / provide pressure control due to loss of coolant or coolant contraction (described in Section 6.1.2).

The key performance and design parameters for ASF [JD02] are summarised in Table 6.2-7. A simplified schematic of the ASF [JD02] and key SSC contributing to its operation is illustrated in Figure 6.2-1.

Table 6.2-7: Key Design & Performance Parameters for ASF [JD02]

Parameter	Value
Injection flow rate (per train)	{REDACTED}
Required boron concentration for CZP	{REDACTED}
Response time (from initiation to first boron delivery to DVI nozzles)	21 s
Target reliability (probability of failure on demand (PFD))	1 x 10^{-3}

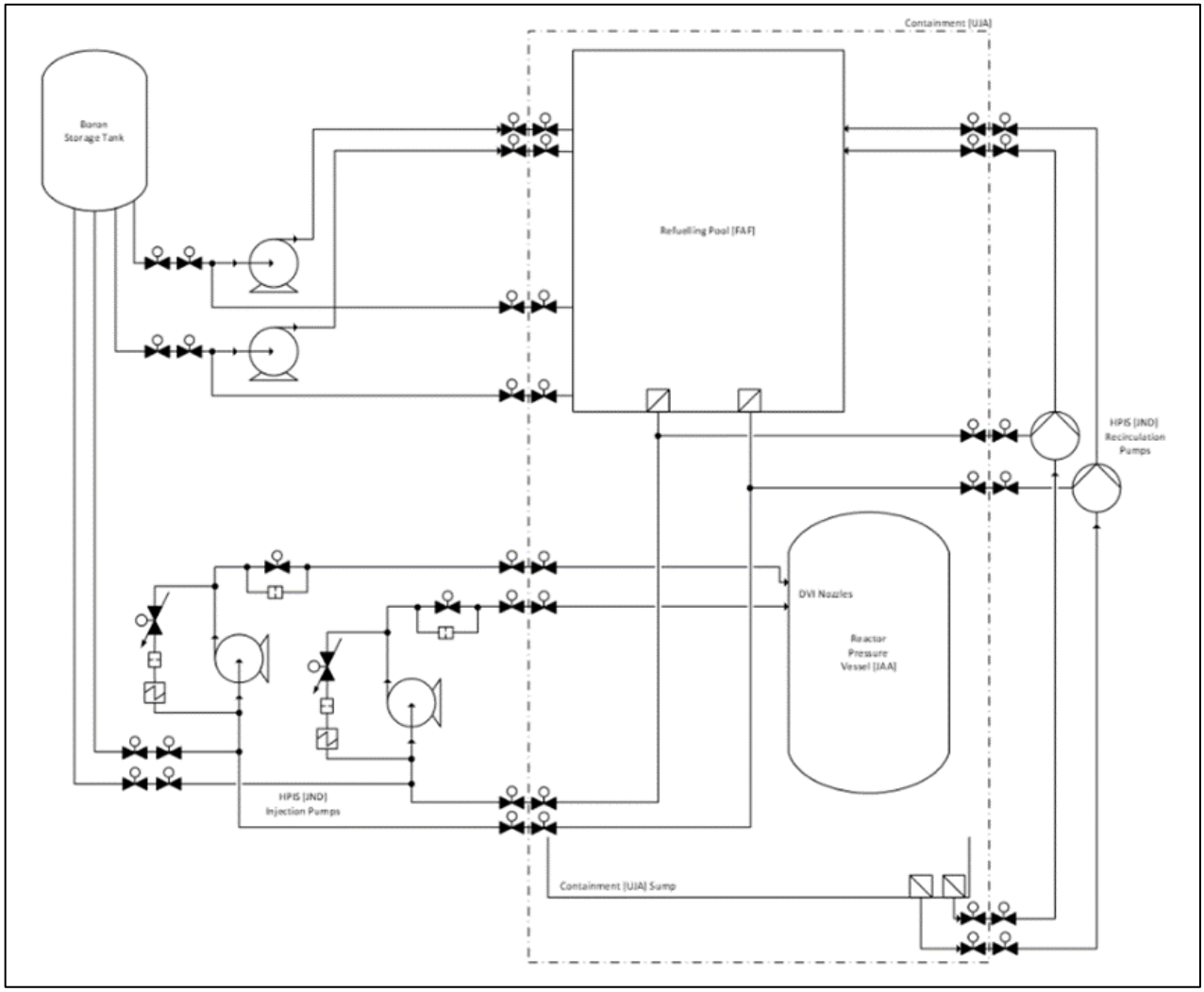


Figure 6.2-1: Simplified Schematic of ASF [JD02]

The developing layout of the key SSC supporting ASF [JD02] operation is summarised in [11]. Each of the key sub-systems delivering ASF [JD02] are located within the hazard shield and on the aseismic bearing to provide protection against external hazards.

Separation and segregation of redundant trains is adopted within the layout to ensure ASF [JD02] can deliver its function in the event of an internal hazard, examples include:

- The two HPIS [JND] trains are entirely segregated by a partition wall, within the Safety Systems Block [UJT].

- Supply and return pipelines from the HPIS [JND] to the Containment System [JMA] are routed from the Safety Systems Fluids Block [UJT] through Level 2, removing the need for pipework to pass through the seismically isolated slab and improving the ease of construction, maintenance, and decommissioning.

Further description of ASF [JD02], including detail of the associated sub-systems and components, is provided in the ASF SMDD [25].

6.2.2.4 Materials

The description and justification of materials used for Class 2 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.2.2.5 Interfaces with Supporting Systems

ASF [JD02] is designed to operate alongside the PDHR [JN02] that provides CoFT. ECC [JN01] is only compatible with Scram [JD01] and does not operate with ASF [JD02].

ASF [JD02] is automatically initiated by the RPS2 [JRA20] in response to instrument trips which indicate faulted conditions, see section 6.2.2.7. It is also capable of being initiated manually by an operator in the MCR in response to an alarm or observed progression to a faulted condition.

ASF [JD02] components that require power are supplied from the grid or Main Generator [MK] (house load operation). During a LOOP, power to the ASF [JD02] components is supplied from the standby AC power supplies in the High Voltage Power Generation System [BDV], with the Low Voltage Uninterruptible DC Supply System for Safety Services [BQ] providing power (from batteries) for any C&I and actuation that is required during the start-up of the standby AC power. The electrical power systems are described further in E3S Case Version 2, Tier 1, Chapter 8: Electrical Power System [12].

6.2.2.6 SSC Operation

6.2.2.6.1 Normal Operation

The Reactor Island Operating Philosophy [13] 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 [14].

During Operating Mode 1 (power operation), ASF [JD01] will be on standby, monitoring plant parameters to trip when traversing outside of the operational set points, and if Scram [JD01] has failed. During Operating Mode 2 (start-up) as the rods are gradually withdrawn to provide reactivity addition, ASF [JD02] will also be tripped if the flux parameters measured by Scram [JD01] continue to exceed limits.

During Operating Mode 3 (hot standby), Operating Mode 4a (hot shutdown – steaming), 4b (hot shutdown – non-steaming), 5a (cold shutdown – pressurised), and 5b (cold shutdown – depressurised), ASF [JD02] is not required as the control rods are fully inserted, providing reactivity hold down. During Operating Mode 6a (refuelling with reduced water level above fuel) and 6b (refuelling with reduced water level above fuel at nominal full), the CRDMs will be removed to access in the RPV [JAA] internals and ASF [JD02] is not required.

6.2.2.6.2 Operation during Faults

The primary function of ASF [JD02] is to provide a diverse role in the CoR during plant faulted operations. Following a monitored parameter reaching a trip condition, the RPS2 [JRA20] automatically initiates ASF [JD02] phase 1. Manual initiation of ASF [JD02] is also possible from the MCR.

ASF [JD02] phase 2 is triggered by the PDHR [JN02] pressuriser level low trip, to ensure that ASF [JD02] is initiated prior to PDHR [JN02] tripping of HPIS [JND], to avoid reactivity increase from the addition of cold Refuelling Pool [FAF] water.

During a LOCA the CVCS [KB] is also isolated to prevent boron dilution by the CVCS charging pumps or ion exchange resins.

Specific operational responses to fault conditions are described in [25].

6.2.2.7 Instrumentation & Control

All ASF [JD02] functionality can be automatically initiated without reliance on the operator. This is achieved through a series of automatic control and instrumentation functions, described in [25].

ASF [JD02] places several trip functions onto the Reactor Control and Protection System [JY] for initiation, specifically the RPS2 [JRA20]. 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 SCR, enabling the manual initiation of 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 Reactor Control and Protection System [JY] and allocation of safety categorised functional requirements from the ASF [JD02] is described further in E3S Case Version 2, Tier 1, Chapter 7: Instrumentation & Control [15], with further details provided in ASF SMDD.

Independent initiation parameters and sensors are used between Scram [JD01] and ASF [JD02] to achieve diversity. Scram [JD01] can be initiated by two diverse control systems, RPS1 [JRA10] and DPS [JQA], whereas the ASF [JD02] is initiated by the RPS2 [JRA20].

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 Scram [JD01] will have had the opportunity to be successfully actuated first.

6.2.2.8 Monitoring, Inspection, Testing and Maintenance

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

The EMIT activities for ASF [JD02] are defined as TLA within the RR SMR requirements management database, and cover safety derived tasks (ISI, reliability derived tasks (RCM/preventative maintenance), and industry best practice/OPEX (EPRI PMBD).

6.2.2.9 Radiological Aspects

No significant radiological aspects associated with the ASF [JD02] operation have been identified. 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 operator exposure.

6.2.2.10 Performance and Safety Evaluation

6.2.2.10.1 Compliance with Safety Categorised Functional Requirements

Verification strategies for ASF [JD02] and associated sub-systems to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements primarily include performance analysis using RELAP5-3D and VIPRE-01 codes, with core flow and boron mixing rig testing to validate analysis.

Performance analysis demonstrates that ASF [JD02] can be successfully initiated within required timescales to deliver its safety functions for all fault conditions at RD7/DRP1. The output of performance analysis and margin to acceptance criteria for ASF [JD02] are presented in [25], with the suite of performance analysis for bounding fault conditions that place safety categorised functional requirements on ASF [JD02] presented in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.2.2.10.2 Compliance with Non-Functional System Requirements

A summary of the compliance for non-functional system requirements allocated to ASF [JD02] are summarised in Table 6.2-8. Further details are provided in [23] and [25].

Table 6.2-8: ASF [JD02] Non-Functional System Requirements Compliance

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD02-R-1709	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis internal hazards.	HPIS [JND] and EBIS [JDK] both have 1oo2 redundant trains (except the passive boron tank) which are segregated such that a single internal hazard is unlikely to result in CCF.
JD02-R-1710	Class 1 and Class 2 measures provided for DBC-2, DBC-3 and DBC-4 shall deliver their functions following design basis external hazards.	All SSCs which support ASF [JD02] are contained within and supported upon the Hazard Shield and Aseismic Bearing respectively. ASF [JD02] is designed with redundant trains which are segregated such that a single external hazard in unlikely to result in CCF of more than one train PDHR [JN02].
JD02-R-1711	Safety measures shall deliver the defined success criteria.	Performance analysis demonstrates that the ASF [JD02] successfully removes heat to deliver its safety function.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD02-R-1692	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.	HPIS [JND] and EBIS [JDK] both have 1oo2 redundant trains (except the passive boron tank) which are segregated such that a single internal hazard in unlikely to result in CCF. RPS2 [JRA20] instrumentation used to initiate ASF [JD02] is to have 2oo3 redundancy to ensure fault is detected following failure of a single instrument, whilst mitigating spurious trips. ASF [JD02] is functionally diverse to Scram [JD01].
JD02-R-1694	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.	ASF [JD02] is designed to deliver its functions in response to the most onerous initial operating states. Performance analysis which supports safety measure design uses a combined approach including a best-estimate analysis method with conservative assumptions, including initial and boundary conditions.
JD02-R-1695	The design shall fail to a safe state where practicable	Valves that move position in response to a safety demand from the C&I systems or are in pipework that supports successful ASF [JD02] operation, are specified to fail to a safe position upon loss of power. RCPs include flywheels, which provide an elongated coast-down following a loss of primary flow fault, to facilitate NC coolant flow to support ASF [JD02] operation. Sensors fail to a trip state, which places the associated RPS logic train into a tripped state.
JD02-R-1697	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.	For each bounding design basis fault, ASF [JD02] ensures selected trip parameters relate directly to the fault, where practicable, in order to provide rapid response.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JD02-R-1699	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.	For all design basis fault conditions, ASF [JD02] initiates automatically without operator action.
JD02-R-1700	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.	The design of ASF [JD02] ensures no essential services are needed from on-site mobile equipment for 72 hours or from off-site for 7 days.
JD02-R-1701	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.	ASF [JD02] is designed to interface with offsite equipment in deliver of its categorised functions, primarily via electrical power connections.
JD02-R-1702	Human-system interfaces shall be designed for optimised and reliable human performance, designed according to ergonomic principles.	Human factors assessment ensure integration through the design process, including human factors checklists, allocation of function, task analysis and human reliability analysis.

6.2.2.10.3 ALARP, BAT, Secure by Design and Safeguards by Design

Key ASF [JD02] design decisions made with respect to ensuring overall risks are reduced to ALARP, BAT, secure by design and safeguards by design include:

- The use of HPIS [JND] to inject boron into the RCS [JE] 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.
- The use of a boron storage tank over options such as borated accumulators or a powdered boron tank, providing relative safety benefits including reduced complexity and reduced potential for boron crystallisation or undissolved boron powder leading to failure of valves or pumps. Additional boron tanks only marginally improve PFD, whilst a single tank is in line

with RGP and reduces the inventory of chemicals and waste (both during operation and decommissioning).

- Boron mixing in the Refuelling Pool [FAF], which is a more robust way of ensuring a minimum boron concentration compared to metering. It also reduces the volumes of solid and borated waste produced throughout the power station's lifetime.

More detailed information on design decisions is presented in the ASF SMDD [25] and associated design decision files.

6.3 Safety Features for Stabilisation of the Molten Core

6.3.1 System and Equipment Functions

The RR SMR incorporates an In-Vessel Retention (IVR) function, to ensure that in a severe accident with core damage (DEC-B), corium can be retained within the RPV [JAA]. This function contributes to practical elimination of several highly energetic ex-vessel severe accident phenomena.

The IVR supports the FSF of CoRM, achieved through the Containment Safety Measure (CSM) [JM01], which is described holistically in section 6.4.1.

The function places requirements on several systems, including the RPV [JAA], RPV internals [JAC], Lower Dome Civil Structures [UJA], Refuelling Pool [FAF], and the dedicated Reactor Vessel Cavity Injection System (RVCIS) [JNM].

6.3.2 Design Bases

The design bases for the IVR function, including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

IVR supports the safety category C function to flood the RPV Cavity in DEC-B accidents. The RVCIS [JNM] is the dedicated system that supports the IVR function and is classified as safety class 3, except for the valves and lines that provide isolation of the Refuelling Pool [FAF], which are safety class 1. The other SSCs that contribute to the IVR function have a higher safety classification as they deliver other higher category functions during other modes of operation.

No environment, security, safeguards, or seismic performance classification is assigned at RD7/DRP1.

6.3.3 Description

The IVR function is achieved by flooding the reactor cavity, and transferring heat from corium, via the RPV and coolant, to the containment atmosphere. There are two phases to IVR; an initial phase which is required to flood the RPV cavity prior to core relocation, and a recirculation phase which maintains the flood-up level in the RPV cavity by replacing any coolant lost from boiling.

Key sub-systems that are relied upon by the IVR function include the:

- RPV [JAA], which transfers heat from the corium into the coolant, and retains the corium
- RPV insulation [JAA], which acts as a flow channel device during IVR to increase the margin to critical heat flux. Additionally, the RPV support structure has been engineered to vent steam from the RPV cavity into the containment atmosphere
- RPV Internals [JAC], which delay core relocation to the lower head, and once a molten pool has formed, to increase the thickness of the light metallic layer reducing the challenge to RPV integrity.
- Lower Dome Civil Structures System [UJA], including the containment sump which contains coolant for the on-going decay heat removal phase of IVR, and the RPV Cavity [UJA] which contains coolant during both phases of IVR

- Refuelling Pool [FAF], which is used as the coolant source for initial flood-up and interfaces with the RVCIS [JNM] initial flood-up train inlets

- The depressurisation systems (ADS [JNF] and the Reactor Coolant Pressure Relief System [JEG]) and the RVCIS [JNM], described in section 6.4.6.2

The only dedicated system that supports IVR is the RVCIS [JNM], which has four lines in total; two connecting the Refuelling Pool [FAF] with the RPV Cavity [UJA] that provide coolant as part of the initial flood-up phase of IVR, and two lines that connect the Containment Sump [UJA] with the RPV Cavity [UJA] to provide coolant for the recirculation phase of IVR.

A simplified schematic of the SSCs delivering the IVR function is illustrated in Figure 6.3-1.

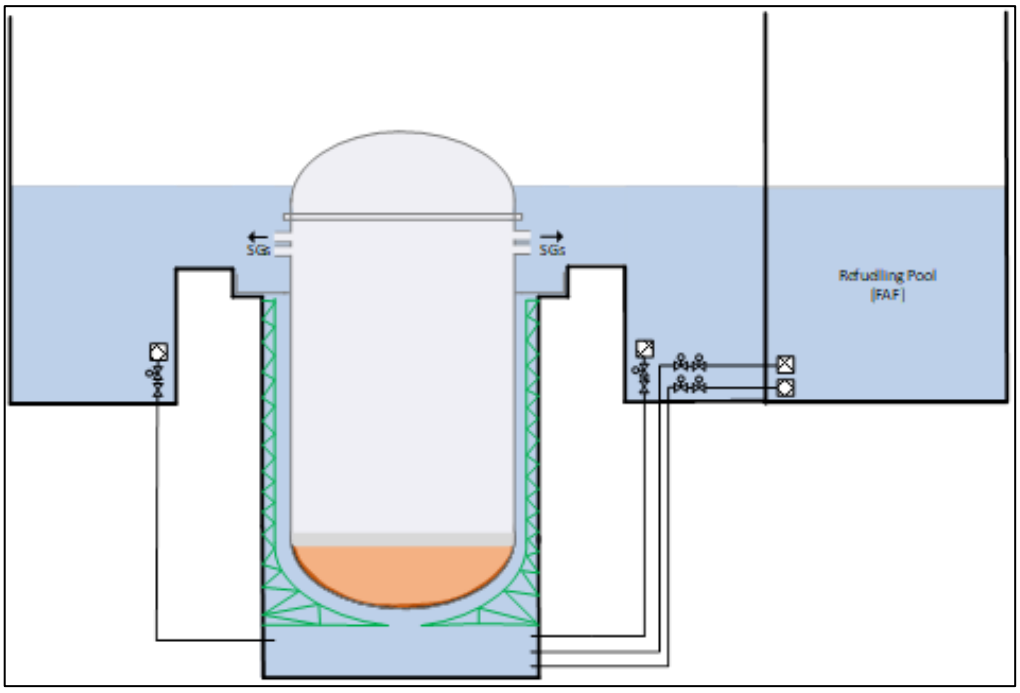


Figure 6.3-1: Simplified Schematic of the IVR Function

Further details of the IVR function and the RVCIS [JNM] are described in the IVR and RVCIS System Design Description (SDD) [26].

6.3.4 Materials

The description and justification of materials used for safety classified SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.3.5 Interfaces with Supporting Systems

The IVR function interfaces with C&I systems to provide monitoring and alarms, see section 6.3.7.

6.3.6 System and Equipment Operation

The initial flood-up phase of IVR can be initiated by an operator as part of the Severe Accident Management Guidelines (SAMGs), primarily in response to a high core exit temperature. When

initiated, the four valves on the two initial flood-up lines of the RVCIS open fully providing coolant from the Refuelling Pool [FAF] to the RPV Cavity [UJA] via gravity.

The initial flood-up lines provide coolant to the RPV Cavity [UJA] to flood the cavity prior to core relocation using gravity flow from the Refuelling Pool [FAF]. The recirculation lines provide on-going supply of coolant to the RPV Cavity [UJA], to initially replace any water that has boiled , and long-term cooling via NC.

6.3.7 Instrumentation and Control

To support the safe operation and control of the IVR function, the Reactor Control and Protection System [JY] will monitor a range of key system parameters and provide indication of their level or status to the operator in the MCR and in the SCR. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. These are described in [26].

The IVR function is part of the CSM [JM01] and is safety category C, therefore is allocated to the Severe Accident Management System (SAMS) [JRQ20] (see section for all CSM [JM01] functions).

6.3.8 Examination, Monitoring, Inspection and Testing

The overall EMIT philosophy for the CSM [JM01] is described in section 6.4.1.8. The initial philosophy for the RVCIS [JNM] is that lines will be maintained as part of shutdown when the Refuelling Pool [FAF] is empty. Moving parts (valves) are located within the containment sump for accessibility.

6.3.9 Radiological Aspects

The function of the IVR is to prevent highly energetic ex-vessel phenomena, contributing towards preventing the release of material from containment in the unlikely event of a core melt accident.

6.3.10 Performance and Safety Evaluation

The performance and safety evaluation for the CSM [JM01] is described in section 6.4.1.10.

6.4 Containment and Associated Systems

6.4.1 Containment Safety Measure

6.4.1.1 System and Equipment Functions

The function of the CSM [JM01] is to avoid the unplanned release of radioactive material from the RCS [JE] and the Reactor System [JA] during normal and all faulted operations. The CSM [JM01] provides the FSF of CoRM in response to both DBCs and DECs.

CSM [JM01] relies upon different sets of SSC to provide CoRM following different PIEs. These are referred to as 'variants' of the CSM [JM01] within the fault schedule. The variants of CSM [JM01] and their associated SSC defined at RD7/DRP1 include:

- CSM [JM01] variant 1 – duty containment
    - Reactor System [JA], RCS [JE], Containment System [JMA], Containment Heating, Ventilation, Air Conditioning (HVAC) [KLA]
- CSM [JM01] variant 2 – LOCA containment
    - Reactor System [JA], RCS [JE], Containment System [JMA]
- CSM [JM01] variant 3 – fully isolated containment
    - Reactor System [JA], RCS [JE], Containment System [JMA], Hydrogen Reduction System (HRS) [JMT]
- CSM [JM01] variant 4 – severe accident containment
    - Containment System [JMA], HRS [JMT], Fuel Pool Cooling System [FAK], Reactor Coolant Pressure Relief System [JEG], CSCS [JNA], ADS [JNF], LUHS [JNK], RVCIS [JNM]

6.4.1.2 Design Bases

6.4.1.2.1 Functional Requirements

Safety categorised functional requirements specified for the CSM [JM01] based on the HLSFs they deliver are presented in Table 6.4-1 based on [27].

Table 6.4-1: CSM [JM01] Safety Categorised Functional Requirements

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JM01-R-1344	The Containment Safety Measure [JM01] variant 1 shall form a leak-tight barrier around the RCS [JE] and the Reactor System [JA].	1 to 5b	C

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JM01-R-1346	The Containment Safety Measure [JM01] variant 1 shall reduce airborne activity inside Containment System [JMA].	1 to 5b	C
JM01-R-1345	The Containment Safety Measure [JM01] variant 1 shall monitor conditions inside Containment System [JMA].	1 to 5b	C
JM01-R-1341	When relevant faults occur, the Containment Safety Measure [JM01] variant 2 shall form a leak-tight barrier around the RCS [JE] and the Reactor System [JA].	1 to 5b	B
JM01-R-1342	When relevant faults occur, the Containment Safety Measure [JM01] variant 2 shall isolate the Containment System [JMA] on demand.	1 to 5b	B
JM01-R-1343	When relevant faults occur, the Containment Safety Measure [JM01] variant 2 shall monitor conditions inside Containment System [JMA].	1 to 5b	C
JM01-R-1337	When relevant faults occur, the Containment Safety Measure [JM01] variant 3 shall form a leak-tight barrier around the RCS [JE] and the Reactor System [JA].	1 to 5b	A
JM01-R-1338	When relevant faults occur, the Containment Safety Measure [JM01] variant 3 shall isolate the Containment System [JMA] on demand.	1 to 5b	A
JM01-R-1339	When relevant faults occur, the Containment Safety Measure [JM01] variant 3 shall reduce hydrogen concentrations inside Containment System [JMA].	1 to 5b	B
JM01-R-1340	When relevant faults occur, the Containment Safety Measure [JM01] variant 3 shall monitor conditions inside Containment System [JMA].	1 to 5b	C
JM01-R-1289	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall form a leak-tight barrier around the RCS [JE] and the Reactor System [JA].	1 to 5b	C
JM01-R-1312	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall isolate the Containment System [JMA] on demand.	1 to 5b	C
JM01-R-1290	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce hydrogen concentrations inside Containment System [JMA].	1 to 5b	C

Requirement ID	Functional Requirement	Mode(s) of Operation	Safety Category
JM01-R-1292	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall remove heat from Containment System [JMA] to the ultimate heat sink.	1 to 5b	C
JM01-R-1291	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce the Reactor Plant [J] pressure.	1 to 5b	C
JM01-R-1247	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall retain corium in the Reactor Vessel Assembly [JAA].	1 to 5b	C
JM01-R-1293	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall monitor conditions inside Containment System [JMA].	1 to 5b	C
JM01-R-1328	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce the pressure inside Containment System [JMA].	1 to 5b	C
JM01-R-1313	When relevant faults occur, the Containment Safety Measure [JM01] variant 4 shall reduce the quantity of airborne radioactive material inside Containment System [JMA].	1 to 5b	C

CSM [JM01] variant 1 provides the final barrier to provide CoRM during normal operation (DBC-1 and DBC-2i), therefore the functions performed are safety category C.

CSM [JM01] variant 2 provides the leaktight barrier and isolation to provide of CoRM during frequent faults (DBC-2ii and DBC-3i) where consequences are low, therefore performing a safety category B function.

CSM [JM01] variant 3 provides the leaktight barrier, isolation of containment, and hydrogen mitigation to provide CoRM during infrequent faults and frequent faults with failure of the first protective measure (DBC3ii and DBC-4), where consequences are high due to some fuel failure, therefore performing a safety category A function.

CSM [JM01] variant 4 provides the mitigative measure to provide CoRM during severe accidents (DEC-B), where the RCS boundary is no longer intact and fuel melt has occurred, therefore performing a safety category C function.

The relevant PIEs that the CSM [JM01] is claimed against are listed in [27].

The safety categorised functional requirements for the CSM [JM01] are flowed down and allocated to relevant sub-systems and/or components in [28]. Non-functional performance requirements associated with the safety categorised functional requirements are allocated in [27].

No environment, security or safeguards functional requirements are assigned at RD7/DRP1.

6.4.1.2.2 Non-Functional System Requirements

Non-functional system requirements are allocated to the CSM [JM01] based on the E3S design principles as described in E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2], summarised in Table 6.4-2.

Table 6.4-2: CSM [JM01] Non-Functional System Requirements

Requirement ID	Non-Functional System Requirement
JM01-R-1711	For each PIE, the design shall provide safety measures at each level of defence in depth where reasonably practicable
JM01-R-1713	Safety measures shall deliver the defined success criteria.
JM01-R-1716	The design shall employ the hierarchy of controls
JM01-R-1718	The design shall fail to safety
JM01-R-1719	The design shall have large margins to failure and long time constants so that key parameters deviate only slowly from their desired values.
JM01-R-1720	Failure modes shall be gradual and predictable.
JM01-R-1722	Safety measure design definition shall avoid complexity by requiring the fewest number of actions to deliver the safety outcome
JM01-R-1723	Safety measures shall be designed to be highly reliable, with a baseline safety measure probability of failure on demand for demand-based measures or failure frequency for continuously-operating measures expectation of: Safety class 1: 1E-03 to 1E-05 per year Safety class 1: 1E-03 to 1E-05 per demand Safety class 2: 1E-02 to 1E-03 per year Safety class 2: 1E-02 to 1E-03 per demand Safety class 3: 1E-01 to 1E-02 per year Safety class 3: 1E-01 to 1E-02 per demand
JM01-R-1724	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.
JM01-R-1725	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
JM01-R-1726	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall feature redundancy
JM01-R-1727	Redundant trains of safety measures shall be segregated from one another
JM01-R-1728	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on the correct performance of other equipment.

Requirement ID	Non-Functional System Requirement
JM01-R-1729	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the presence of failures or unintended operation of other equipment, where this could exacerbate the consequences, or otherwise make the fault more severe.
JM01-R-1730	Class 1 and Class 2 safety measures shall feature diverse means of initiation between the two safety measures, for sequences where both safety measures require automatic initiation.
JM01-R-1731	Class 1 and Class 2 safety measures shall feature a diverse on-site supply of essential services between measures, for sequences where both measures require the same essential service.
JM01-R-1732	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.
JM01-R-1733	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.
JM01-R-1734	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the presence of a single failure.
JM01-R-1735	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the worst normally permitted configuration of equipment outages for maintenance, test, or repair.
JM01-R-1736	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions with diverse means of initiation to the extent reasonably practicable, which shall be via the use of different variables, when the measure requires automatic initiation.
JM01-R-1737	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
JM01-R-1738	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions with a supply of on-site essential services diverse from sources claimed for DBC, for sequences where the same essential service is needed for DEC functions and no on-site diversity exists for DBC.
JM01-R-1739	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions following the crash of a commercial aeroplane.
JM01-R-1740	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.

Requirement ID	Non-Functional System Requirement
JM01-R-1741	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions without reliance on essential services supplied from on-site mobile equipment for 24 hours or from off-site for 7 days.
JM01-R-1742	For DEC-B, safety measures shall be designed to deliver their functions following design basis internal and external hazards.
JM01-R-1743	For DEC-B, safety measures shall be designed to deliver their functions without reliance on operator action for at least 12 hours, ideally 24 hours.
JM01-R-1744	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.
JM01-R-1745	Defence against common cause failure shall be provided though inclusion of diversity within and between safety measures claimed in a sequence where reasonably practicable
JM01-R-1746	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.
JM01-R-1747	Redundant connection points shall be provided for interfaces between safety measures and off-site equipment supplying water, electrical power and any other consumable media used in delivery of a categorised function.
JM01-R-1750	[Process] For each hazard, the design shall include dedicated SSCs to prevent escalation of hazards to induce faults and to prevent damage to classified SSCs that may be claimed against any induced initiating event where reasonably practicable.
JM01-R-1751	The design shall provide monitoring and alerting to give forewarning of relevant external hazards so that administrative processes may prevent initiating events from occurring, minimise their magnitude, and/or minimise the potential for consequences should an initiating event occur.
JM01-R-1753	Classified systems and components, as well as people shall be segregated from sources of internal hazards.
JM01-R-1754	Classified systems and components, as well as people shall be segregated from external hazards.
JM01-R-1761	The layout and design shall facilitate accident management and emergency response
JM01-R-1767	The Containment shall maintain its structural integrity for design basis conditions and design extension conditions, including a double-ended guillotine failure of a main leg of the RCS and during severe accidents.
JM01-R-1768	The containment system shall incorporate features to confine the location of any postulated molten core material and prevent its uncontrolled spreading around the containment environment.

Requirement ID	Non-Functional System Requirement
JM01-R-1769	The containment system design shall contain features to reduce the amounts of fission products that could be released to the environment in accident conditions
JM01-R-1770	The size and number of containment penetrations shall be reduced to the extent reasonably practicable
JM01-R-1771	Containment penetrations shall meet or exceed the same design requirements as the containment structure itself
JM01-R-1809	The design shall provide criticality safety through the Double Contingency Approach.
JM01-R-1828	The design of pressure discharge systems shall not enable the creation of an explosive atmosphere
JM01-R-1881	The design definition of Safety Class 1 and Safety Class 2 safety measures shall detail the minimum amount of operable equipment, actions to be taken in the event of deviations from the operational limits and conditions and the time allowed to complete these actions.
JM01-R-1883	Safety measures shall not experience unplanned initiation in the course of normal operations.
JM01-R-1887	Safety class 1 and safety class 2 structures, systems and components shall apply nuclear specific codes and standards where available.
JM01-R-1888	Safety class 3 structures, systems and components shall apply either nuclear specific or other appropriate industrial codes and standards.
JM01-R-1903	Safety measures shall be designed to achieve numerical risk targets.
JM01-R-1906	Safety systems shall perform any safety categorised functions passively.

6.4.1.2.3 E3S Classification

Safety Classification

The variants of the CSM [JM01] provide safety category A, B and C functions, and are classified in accordance with the E3S categorisation and classification methodology outlined in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives & Design Rules [2], The safety classification of the systems and components delivering the CSM [JM01] are specified in relevant sub-sections of this report.

Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

Seismic Performance Classification

The seismic performance classification will principally be SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.4.1.3 Description

The CSM [JM01] allocates E3S requirements to a range of SSCs that deliver its functions, described for each CSM variant in section 6.4.1.1. Each of these sub-functions delivered by the CSM [JM01] are summarised below. The baseline key performance and design parameters for SSC delivering the sub-functions are described in the referenced sub-sections of this report.

Containment System

The Containment System [JMA] forms a leak tight pressure boundary around the RCS [JE]. The Containment System [JMA] is considered the final barrier to confine radioactive material, after the fuel pellet, the fuel cladding tubes, and the pressure boundary of the RCS [JE].

The containment free air volume is sufficient to withstand the applicable loads during faults. The containment internal layout is designed to be open to support natural convection heat removal in faults and minimise accumulation of combustible gases during severe accidents.

The Containment System [JMA] is described further in section 6.4.2.

Containment Isolation

Fluid systems which pass through containment include isolation valves. Five generic types of fluid system penetrations have been defined for the different fluid system configurations expected to penetrate the Containment System [JMA]. The components supporting containment isolation are designed to perform their function across the range of environmental conditions that might prevail during DBCs and DECs.

Containment isolation is described further in section 6.4.6.1.

Containment Heat Removal and Depressurisation

The containment heat removal subfunction prevents the Containment System [JMA] and SSC required during faults from exceeding their pressure and temperature limits. Both passive (using PCC heat exchangers) and active (using CSCS [JNA] and Fuel Pool Cooling System (FPCS) [FAK]) heat removal methods are independently capable of removing heat from containment.

Containment heat removal and depressurisation is described further in section 6.4.4.

Severe Accident Depressurisation

The CSM [JM01] depressurises the RCS [JE] during DEC-B fault sequences to mitigate high pressure melt ejection and direct containment heating that could challenge containment integrity. Depressurisation is also beneficial for interrupting the natural circulation of hot gases in the RCS [JE], which could lead to creep rupture of the SG tubes and containment bypass. There RR SMR includes two methods to depressurise the primary circuit, including manual depressurisation using the Reactor Coolant Pressure Relief System [JEG] High Temperature Overpressure Protection (HTOP) valves, or manual depressurisation using the ADS [JNF].

Severe accident depressurisation is described further in section 6.4.6.2

Hydrogen Management

The primary means of preventing hydrogen explosions/combustion which could challenge containment integrity is the large open free air volume of the Containment System [JMA] and the intentional layout of SSCs to eliminate corridors and enclosed spaces, where practicable. Furthermore, the HRS [JMT] utilises passive autocatalytic recombiners (PARs) positioned around containment to recombine hydrogen and oxygen to water.

Hydrogen management is described further in section 6.4.5.

In-Vessel Retention

The IVR function ensures the retention of molten corium in the RPV during a severe accident with core melt (DEC-B). This is described further in section 6.3.

Airborne Radioactive Material Reduction

The RR SMR reduces the inventory of radioactive material in the containment atmosphere during normal operation and faulted conditions through Containment HVAC [KLA], natural phenomena (NC, condensation, and deposition), and intermittent spray by the containment cooling and spray function (CCSF).

Airborne radioactive material reduction is described further in section 6.6.

Layout

The developing layout of SSC supporting CSM [JM01] operation is summarised in [11]. Each of the key sub-systems delivering the CSM [JM01] are located within the hazard shield and on the aseismic bearing to provide protection against external hazards.

Separation and segregation are adopted within the layout to ensure the CSM [JM01] can deliver its function in the event of an internal hazard, examples include:

- Coupled LUHS [JNK] tanks are spatially segregated and contained within the buttresses of the Interspace [UJB], meaning an internal blast (e.g., from an accumulator) can only damage a single train of the LUHS heat removal pathway
- The two means of providing severe accident depressurisation, the HTOP valves and the ADS valves, are physically separated from each other

Further description of the CSM [JM01] safety measure, including detail of the associated sub-systems and components, is provided in the CSM SMDD [29].

6.4.1.4 Materials

The description and justification of materials used for safety classified SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.4.1.5 Interfaces with Supporting Systems

Containment isolation is automatically initiated by the Reactor Control and Protection System [JY], see section 6.4.1.7.

Severe accident depressurisation includes features which are partially automatically initiated, including the LP EBD (within the ADS [JNF]) which open automatically when the RCS pressure exceeds set limits.

Variants 2 to 4 of the CSM [JM01], which operate during faults, are designed to avoid active operations which require continuous AC power where practicable, with no continuous AC power requirements for the primary means of achieving any of the CSM [JM01] functions. DC power demands are limited to actuators and associated with initiation of CSM [JM01] functions. These power demands are supplied using the Low Voltage Uninterruptible DC Supply System for Safety Services [BQ], described further in E3S Case Version 2, Tier 1, Chapter 8: Electrical Power System [12].

During CSM [JM01] variant 4, the CSCS [JNA] pumps, which can provide the secondary means of achieving the CSM [JM01] Heat Removal function, require a continuous AC power source. The power demands of the CSCS [JNA] are supplied using the Low Voltage Essential AC Standby Supply System [BK].

6.4.1.6 System and Equipment Operation

6.4.1.6.1 Normal Operation

The Reactor Island Operating Philosophy [13], 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 Version 2, Tier 1, Chapter 13: Conduct of Operations [14].

All functions within the four CSM [JM01] variants are operator initiated, except for those specified in section 6.4.1.5.

During operating mode 1 (power operation) to 4b (hot shutdown – non-steaming), the main equipment hatch, personal airlocks and the fuel transfer tube will normally be closed. All pipework penetrations will be open or closed as required by the MCR.

During operating mode 5a (cold shutdown – pressurised), the Containment System [JMA] is not required to maintain the containment boundary. Operators and equipment can access containment through the personnel airlocks to enable faster preparation of shutdown activities. The main equipment hatch and fuel transfer tube are normally closed. The personnel airlocks can be opened. All pipework penetrations will be open or closed as required by the MCR.

During operating mode 5b (cold shutdown – depressurised), the Containment System [JMA] is not required to maintain the containment boundary. Operators and equipment can access containment through the personnel airlocks to enable faster preparation of shutdown activities. The fuel transfer tube is normally closed. The main equipment hatch and personnel airlocks can be opened. All pipework penetrations will be open or closed as required by the MCR.

During operating mode 6a (refuelling with reduced water level above fuel), the Containment System [JMA] is not required to maintain the containment boundary. The fuel transfer tube and main equipment hatch are closed. The personnel airlocks can be opened.

During operating mode 6B (refuelling with water level above fuel at nominal full), the Containment System [JMA] is not required to maintain the containment boundary. The fuel transfer tube is open, and the main equipment hatch and personnel airlocks can be open.

6.4.1.6.2 Operation during Faults

CSM [JM01] variants 2 and 3 initiate automatically and primarily require different isolation valve configurations. The Containment isolation LOCA phase initiates on LOW pressuriser level or LOW pressuriser pressure or HIGH containment pressure. The Containment Isolation ECC phase 1 initiates on HIGH HP EBD flow or HIGH HP EBD temperature. The Containment Isolation ECC phase 2 initiates on LOW accumulator level.

CSM [JM01] variant 4, and associated subfunctions including containment isolation, can be initiated manually on entry into severe accident management guidelines.

The primary method of containment heat removal using the PCCS heat exchangers [JNK] and hydrogen reduction using the HRS [JMT] do not require any automatic initiation or operator action to function.

The specific alignment for each SSC delivering the CSM [JM01], and operational responses to specific fault conditions, are described in [29].

6.4.1.7 Instrumentation and Control

CSM [JM01] is reliant on the Reactor Control and Protection System [JY] to provide a series of functions. All safety category A functions are assigned to both the RPS [JRA] and the DPS [JQ]. All the safety category functions are assigned to RPS [JRA]. CSM [JM01] variant 4 provides safety category C functions and are assigned to the SAMS [JRQ20].

The Reactor Control and Protection 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 SCR. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. All post-accident monitoring functions are allocated to the Post-Accident Management System (PAMS) [JRQ10], noting those for CSM[JM01] variant 4 are monitored using the SAMS [JRQ20].

The Reactor Control and Protection System [JY] and allocation of safety categorised functional requirements from the CSM [JM01] is described further in E3S Case Version 2, Tier 1, Chapter 7: Instrumentation & Control [15].

6.4.1.8 Examination, Monitoring, Inspection and Testing

The EMIT activities for the CSM [JM01] are defined as TLA within the RR SMR requirements management database, and cover safety derived tasks (ISI, reliability derived tasks (RCM/preventative maintenance), and industry best practice/OPEX (EPRI PMBD).

Containment leak testing supports the CSM [JM01] by confirming the leak tightness of the containment vessel, penetrations, and isolation valves. Periodic leak rate testing will be carried out during normal operation. By conducting leak rate testing at design pressures, the observed leak rate may then be extrapolated over the range of expected pressures between plant states DBC-1 and DEC-B to estimate the expected leak rate.

Integrated Leak Rate Tests (ILRTs) are carried out for the containment vessel to determine the overall leak rate from the containment boundary. Local Leak Rate Tests (LLRTs) are carried out on penetrations and valves to determine the local leak rate of specific components. Periodic leak rate testing is broken down into three different types, all of which require a different method and different periodicity, described further in [29].

6.4.1.9 Radiological Aspects

The purpose of the CSM [JM01] is to deliver functions to achieve the FSF of CoRM and prevent or mitigate radiological exposures. Radiological consequences for fault sequences are described further in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.4.1.10 Performance and Safety Evaluation

6.4.1.10.1 Compliance with Safety Categorised Functional Requirements

Verification strategies for the CSM [JM01] to demonstrate compliance with its safety categorised functional requirements and associated non-functional performance requirements primarily include performance analysis using GOTHIC and MAAP codes.

Performance analysis demonstrates that the CSM [JM01] can successfully provide key safety functions for all fault conditions considered at RD7/DRP1. The output of performance analysis and margin to acceptance criteria for the CSM [JM01] are presented in [29], with the suite of performance analysis for bounding fault conditions that place safety categorised functional requirements on the CSM [JM01] presented in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [3].

6.4.1.10.2 Compliance with Non-Functional System Requirements

A summary of the compliance for non-functional system requirements allocated to the CSM [JM01] are summarised in Table 6.4-3. Further details are provided in [27] and [29].

Table 6.4-3: CSM [JM01] Non-Functional System Requirements

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1711	For each PIE, the design shall provide safety measures at each level of defence in depth where reasonably practicable	Sufficient defence in depth to achieve CoRM is demonstrated through the fault schedule [3].
JM01-R-1713	Safety measures shall deliver the defined success criteria.	Performance analysis demonstrates that the CSM [JM01] can successfully deliver its safety functions.
JM01-R-1716	The design shall employ the hierarchy of controls	The CSM [JM01] is designed to deliver passive and simple safety where practicable, as described in [29].
JM01-R-1718	The design shall fail to safety	Compliance demonstration ongoing.
JM01-R-1719	The design shall have large margins to failure and long time constants so that key parameters deviate only slowly from their desired values.	Margins demonstrated in safety analysis [3].
JM01-R-1720	Failure modes shall be gradual and predictable.	

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1722	Safety measure design definition shall avoid complexity by requiring the fewest number of actions to deliver the safety outcome	The CSM [JM01] is designed to deliver passive and simple safety where practicable, as described in [29]. Most functions require single valve re-alignments.
JM01-R-1723	Safety measures shall be designed to be highly reliable, with a baseline safety measure probability of failure on demand for demand-based measures or failure frequency for continuously-operating measures expectation of: Safety class 1: 1E-03 to 1E-05 per year Safety class 1: 1E-03 to 1E-05 per demand Safety class 2: 1E-02 to 1E-03 per year Safety class 2: 1E-02 to 1E-03 per demand Safety class 3: 1E-01 to 1E-02 per year Safety class 3: 1E-01 to 1E-02 per demand	Compliance demonstration ongoing.
JM01-R-1724	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.	CSM [JM01] is designed to deliver its functions in response to the most onerous initial operating states. Performance analysis which supports safety measure design use a combined approach including a best-estimate analysis method with conservative assumptions, including initial and boundary conditions.
JM01-R-1725	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.	Redundancy is incorporated throughout the subsystems claimed by CSM [JM01] where practicable to improve resilience to random faults and improve claims on safety measure reliability. Redundancy is also provided following failures consequential upon the initiating event and expected to occur in combination with an initiating event arising from a common cause. See Table 30 and 31 of [29].
JM01-R-1726	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall feature redundancy	

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1727	Redundant trains of safety measures shall be segregated from one another	Separation and segregation are adopted within the layout to ensure the CSM [JM01] can deliver its function in the event of an internal hazard (section 6.4.1.3).
JM01-R-1728	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on the correct performance of other equipment.	Performance analysis demonstrates that the CSM [JM01] can successfully deliver its safety functions.
JM01-R-1729	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions in the presence of failures or unintended operation of other equipment, where this could exacerbate the consequences, or otherwise make the fault more severe.	
JM01-R-1730	Class 1 and Class 2 safety measures shall feature diverse means of initiation between the two safety measures, for sequences where both safety measures require automatic initiation.	Containment isolation is the only Class 1 / 2 measure requiring automatic initiation.
JM01-R-1731	Class 1 and Class 2 safety measures shall feature a diverse on-site supply of essential services between measures, for sequences where both measures require the same essential service.	Compliance demonstration ongoing.
JM01-R-1732	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.	All class 1 measures do not require operator action or are automatic.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1733	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 and Class 2 safety measures shall be conservatively designed to deliver their functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days.	Containment heat removal requires the LUHS [JNK], which over a prolonged period the level could fall to such an extent that further water is required to continue reactor cooling. Long-term cooling solutions are being designed to ensure no essential services are needed from off-site for 7 days.
JM01-R-1734	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the presence of a single failure.	Redundancy for tolerance to single failures is applied to safety class 1 isolation valves.
JM01-R-1735	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions in the worst normally permitted configuration of equipment outages for maintenance, test, or repair.	Compliance demonstration ongoing.
JM01-R-1736	For design basis fault conditions (DBC-2ii/3i/3ii/4), Class 1 safety measures shall be conservatively designed to deliver their functions with diverse means of initiation to the extent reasonably practicable, which shall be via the use of different variables, when the measure requires automatic initiation.	Containment isolation includes diverse initiation.
JM01-R-1737	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.	Severe accident analysis [3] is best estimate with some design margin.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1738	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions with a supply of on-site essential services diverse from sources claimed for DBC, for sequences where the same essential service is needed for DEC functions and no on-site diversity exists for DBC.	Essential services for DECs are diverse from DBCs, section 6.4.1.5.
JM01-R-1739	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions following the crash of a commercial aeroplane.	All SSCs for CSM [JM01] are within the hazard shield.
JM01-R-1740	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions without reliance on operator action in the MCR within 30 minutes, or outside of the MCR within 1 hour, unless personnel are already present in the locality of the place where actions are required.	30-minute delay assumed for all DEC measures requiring operator action.
JM01-R-1741	For DEC-A and DEC-B, safety measures shall be designed on a best estimate basis and deliver their functions without reliance on essential services supplied from on-site mobile equipment for 24 hours or from off-site for 7 days.	At RD7/DRP1 there is no reliance on mobile equipment within 24 hours.
JM01-R-1742	For DEC-B, safety measures shall be designed to deliver their functions following design basis internal and external hazards.	Compliance demonstration ongoing.
JM01-R-1743	For DEC-B, safety measures shall be designed to deliver their functions without reliance on operator action for at least 12 hours, ideally 24 hours.	Severe accident depressurisation and IVR require operator action, designed based on RGP and OPEX, justified in associated decision files (see section 6.4.1.10.3)

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1744	Where a safety measure requires initiation to deliver its function, the triggering variable shall directly relate to the plant condition. Where it is not reasonably practicable to use a directly related variable, the variable chosen shall have a known relationship with the condition caused by the initiating event.	Compliance demonstration ongoing.
JM01-R-1745	Defence against common cause failure shall be provided though inclusion of diversity within and between safety measures claimed in a sequence where reasonably practicable	Compliance demonstration ongoing.
JM01-R-1746	Safety measures shall be designed to interface with off-site equipment to receive supplies of water, electrical power and any other consumable media used in delivery of a categorised function.	Compliance demonstration ongoing.
JM01-R-1747	Redundant connection points shall be provided for interfaces between safety measures and off-site equipment supplying water, electrical power and any other consumable media used in delivery of a categorised function.	Compliance demonstration ongoing.
JM01-R-1750	For each hazard, the design shall include dedicated SSCs to prevent escalation of hazards to induce faults and to prevent damage to classified SSCs that may be claimed against any induced initiating event where reasonably practicable.	Containment is on the aseismic bearing and inside the aircraft hazard protection shield and therefore there is low threat to functions from external hazards.
JM01-R-1751	The design shall provide monitoring and alerting to give forewarning of relevant external hazards so that administrative processes may prevent initiating events from occurring, minimise their magnitude, and/or minimise the potential for consequences should an initiating event occur.	Compliance demonstration ongoing.

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1753	Classified systems and components, as well as people shall be segregated from sources of internal hazards.	Compliance demonstration ongoing.
JM01-R-1754	Classified systems and components, as well as people shall be segregated from external hazards.	Compliance demonstration ongoing.
JM01-R-1761	The layout and design shall facilitate accident management and emergency response	See E3S Case Version 2, Tier 1, Chapter 19: Emergency Preparedness and Response.
JM01-R-1767	The Containment shall maintain its structural integrity for design basis conditions and design extension conditions, including a double-ended guillotine failure of a main leg of the RCS and during severe accidents.	Performance analysis demonstrates that the CSM [JM01] can successfully deliver its safety functions, including LB LOCA.
JM01-R-1768	The containment system shall incorporate features to confine the location of any postulated molten core material and prevent its uncontrolled spreading around the containment environment.	RR SMR includes IVR, see section 6.3.
JM01-R-1769	The containment system design shall contain features to reduce the amounts of fission products that could be released to the environment in accident conditions	RR SMR includes airborne radioactive material reduction, see section 6.6.
JM01-R-1770	The size and number of containment penetrations shall be reduced to the extent reasonably practicable	The RR SMR is designed to minimise penetrations.
JM01-R-1771	Containment penetrations shall meet or exceed the same design requirements as the containment structure itself	Containment penetrations form part of the containment boundary.
JM01-R-1881	The design definition of Safety Class 1 and Safety Class 2 safety measures shall detail the minimum amount of operable equipment, actions to be taken in the event of deviations from the operational limits and conditions and the time allowed to complete these actions.	CSM [JM01] is designed to include the minimum amount of operable equipment.
JM01-R-1883	Safety measures shall not experience unplanned initiation in the course of normal operations.	Design features included to prevent unplanned initiation (electrical isolation).

Requirement ID	Non-Functional System Requirement	Summary of Compliance
JM01-R-1887	Safety class 1 and safety class 2 structures, systems and components shall apply nuclear specific codes and standards where available.	CSM [JM01] is designed to applicable codes and standards outlined in section 6.0.4.
JM01-R-1888	Safety class 3 structures, systems and components shall apply either nuclear specific or other appropriate industrial codes and standards.	CSM [JM01] is designed to applicable codes and standards outlined in section 6.0.4.
JM01-R-1903	Safety measures shall be designed to achieve numerical risk targets.	Assessment against risk targets is presented in the probabilistic safety analysis [3].
JM01-R-1906	Safety systems shall perform any safety categorised functions passively.	Containment heat removal, IVR, airborne radioactive material reduction, and hydrogen reduction are all designed to include passive features.

6.4.1.10.3 ALARP, BAT, Secure by Design and Safeguards by Design

Key CSM [JM01] design decisions made with respect to ensuring overall risks are reduced to ALARP, BAT, secure by design and safeguards by design include:

- Inclusion of manual depressurisation for severe accidents (CSM [JM01] variant 4) to provide an independent means of depressurisation of the RCS at defence in depth level 4, selected based on RGP for PWRs.
- Inclusion of IVR rather than external reactor vessel cooling, providing an additional barrier between radiological release and the environment, and eliminating potential for ex-vessel severe accident phenomena such as molten core-concrete interaction (MCCI), high pressure melt ejection (HPME), direct containment heating (DCH), and ex-vessel steam explosions.
- Use of the Refuelling Pool [FAF] for the IVR water source for initial flood-up, which is shared with the ECC [JN01] phase 2 LOCA water source at defence in depth level 3. This aligns with RGP for independent measures given that operation of the ECC [JN01] phase 1 accumulator injection will delay a core melt and reduce the demand on the IVR. Additionally, successful operation of the ECC [JN01] results in a flooded containment, removing the initial requirement for flooding from IVR. Failure of the structure is very unlikely as it is massive, passive, and seismically qualified, and failure of isolations generally lead to draining into the containment sump, again removing the need for initial flood-up if IVR is demanded.

More detailed information on design decisions is presented in the CSM SMDD [29] and associated design decision files.

6.4.2 Primary Containment System

6.4.2.1 System and Equipment Functions

The function of the Containment System [JMA] is to provide the last barrier of defence in depth to prevent the uncontrolled release of fission products into the environment. The Containment System [JMA] supports the FSF of CoRM during DBCs and DECs (including hazards), achieved as part of the CSM [JM01] described in section 6.4.1. It also provides shielding to workers and the public outside the primary containment.

6.4.2.2 Design Bases

The design bases for the Containment System [JMA], including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

All SSCs associated with the Containment System [JMA] support the safety category A function to confine radioactive substances during both normal and faulted operation. Therefore, all SSCs associated with the Containment System [JMA] that support the confinement function are classified as safety class 1 [30] in accordance with the E3S categorisation and classification methodology outlined in E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2].

No environment, security, or safeguards classification is assigned at RD7/DRP1.

The seismic performance classification will principally be SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.4.2.3 Description

The components of the Containment System [JMA] are described below.

- Containment Vessel Structure [PT250], which provides the main containment boundary, and the structure for other components to attach to. It takes the form of a free-standing welded steel vessel consisting of central a cylindrical section and upper and lower semi-elliptical domes

- Main Equipment Access Hatch [PT251], which provides access to containment during outages for operators and equipment via a simple hinged door. Static elastomeric double seals are used to deliver the leak tight boundary during all other operational and fault states.

- Personnel Airlock [PT252], which provides access to containment during outages for operators and equipment via a cylindrical chamber with hinged doors at either end, both of which open into containment. The doors are designed to withstand most onerous pressures during fault conditions and are interlocked to prevent simultaneous opening of the doors.

- Fuel Transfer Channel [PT253], which provides a leak tight passage between the Refuelling Pool [FAF] inside containment and the Spent Fuel Pool [FAB] outside containment, to allow the transfer of a fuel assembly and any other equipment. Outside of refuelling operations, it contributes to the leak tight containment boundary.

- Pipework Penetration Assemblies [PT260] and isolation valves, which allow fluid system lines to pass through the containment vessel whilst preserving the leak tight boundary. Each penetration includes isolation valves which isolate the flow of fluid through the penetrations.

- Electrical Penetration Assemblies [PT270], which allow electrical control, power, and instrumentation cables to cross the containment boundary whilst preserving the leak tight boundary.

The lower portion of the Containment System [JMA] has two primary interfaces. Externally it is supported by the Containment Support Structure [UWD10], which consists of a concrete centre pedestal and three concrete monolithic support structures equally distributed around the circumference of the containments external lower dome. Inside the containment boundary, the Containment Internal Structures [UJA] form a complete interface with the internal lower dome surface, as well as extend partially upwards onto the first containment ring assembly, which defines the in-containment ground floor level. The Containment Internal Structures [UJA] form the base of the LOCA flood-up sump, as well as extending beyond floor level to serve as a support structure for primary circuit components and systems.

The key performance and design parameters for Containment System [JMA] are summarised in Table 6.4-4. The Containment System [JMA] is illustrated in Figure 6.4-1.

Table 6.4-4: Key Performance and Design Parameters for the Containment System [JMA]

Parameter	**Value**
Design Pressure	{REDACTED
Design Temperature	{REDACTED}
Normal Operating Pressure	{REDACTED}
Normal Operating Temperature	{REDACTED}
Normal Operating Humidity Inside Containment	{REDACTED}
Internal Diameter	{REDACTED}
Internal Height	{REDACTED}
Maximum permissible leakage rate from the containment boundary (at design pressure)	{REDACTED} % of gas volume within containment per day

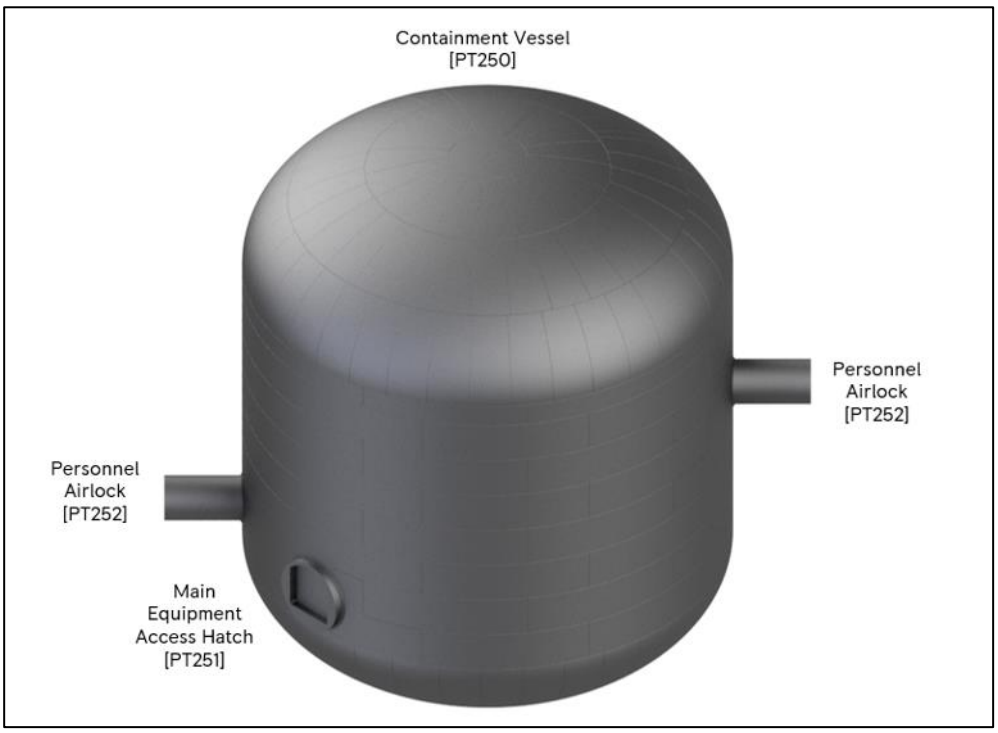


Figure 6.4-1: Containment System [JMA]

Further description of the Containment System [JMA], including detail of the associated and components, is provided in the Containment SDD [30].

6.4.2.4 Materials

The Containment Vessel Structure [PT250] is made from Steel SA738(M) Grade B. It is fabricated by welding ~ 253 individual <60 mm thickness formed plates.

The description and justification of materials used for Class 1 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.4.2.5 Interfaces with Supporting Systems

To support the safe operation and control, the Reactor C&I System [JY] will monitor a range of key system parameters and provide indication of their level or status to the operator in the MCR and in the SCR, these parameters are described in [30].

6.4.2.6 System and Equipment Operation

As described for CSM [JM01] in section 6.4.1.6.

6.4.2.7 Instrumentation and Control

As described for CSM [JM01] in section 6.4.2.5.

6.4.2.8 Examination, Monitoring, Inspection and Testing

As described for CSM [JM01] in section 6.4.1.8

6.4.2.9 Radiological Aspects

As described for CSM [JM01] in section 6.4.1.9.

6.4.2.10 Performance and Safety Evaluation

As described for CSM [JM01] in section 6.4.1.10.

6.4.3 Heading Number Not Used

This section is reserved for secondary containment systems in the IAEA safety report format [31] and is not used by RR SMR.

6.4.4 Containment Heat Removal Systems

6.4.4.1 System and Equipment Functions

The function of the containment heat removal and depressurisation systems is to transfer heat from inside containment to the atmosphere as part of the CSM [JM01], described in section 6.4.1.

The CSM [JM01] uses the following key SSC for heat removal:

- Passive containment heat removal using the PCC heat exchangers and LUHS [JNK] coupled tanks
- Active containment heat removal using the CSCS [JNA] and FPCS [FAK] cooling chains. The cooling chain includes:
    - CSCS [JNA] and FPCS [FAK] to transfer heat from the Containment Sump [UJA] to CCS [KAA]
    - CCS [KAA] to transfer heat from CSCS [JNA] and FPCS [FAK] to ESWS [PBD]
    - ESWS [PBD] to transfer heat from CCS [KAA] to atmosphere

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

6.4.4.2 Design Bases

The design bases for the containment heat removal and depressurisation systems as part of the CSM [JM01], including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

6.4.4.3 Description

Passive Containment Heat Removal

Heat within containment is transferred from the atmosphere to the LUHS [JNK] coolant using the PCC heat exchangers in a passive manner without requiring automatic or operator initiation. The heated coolant in the PCC heat exchangers is transferred to the LUHS coupled tank [JNK] through

NC flow and leaves the system as steam via the LUHS steam duct. The baseline design incorporates three trains with four PCC heat exchangers heat exchangers per train.

The PCC and LUHS arrangement support the ECC [JN01] and are described further in section 6.1.1. A simplified schematic is illustrated in Figure 6.4-2.

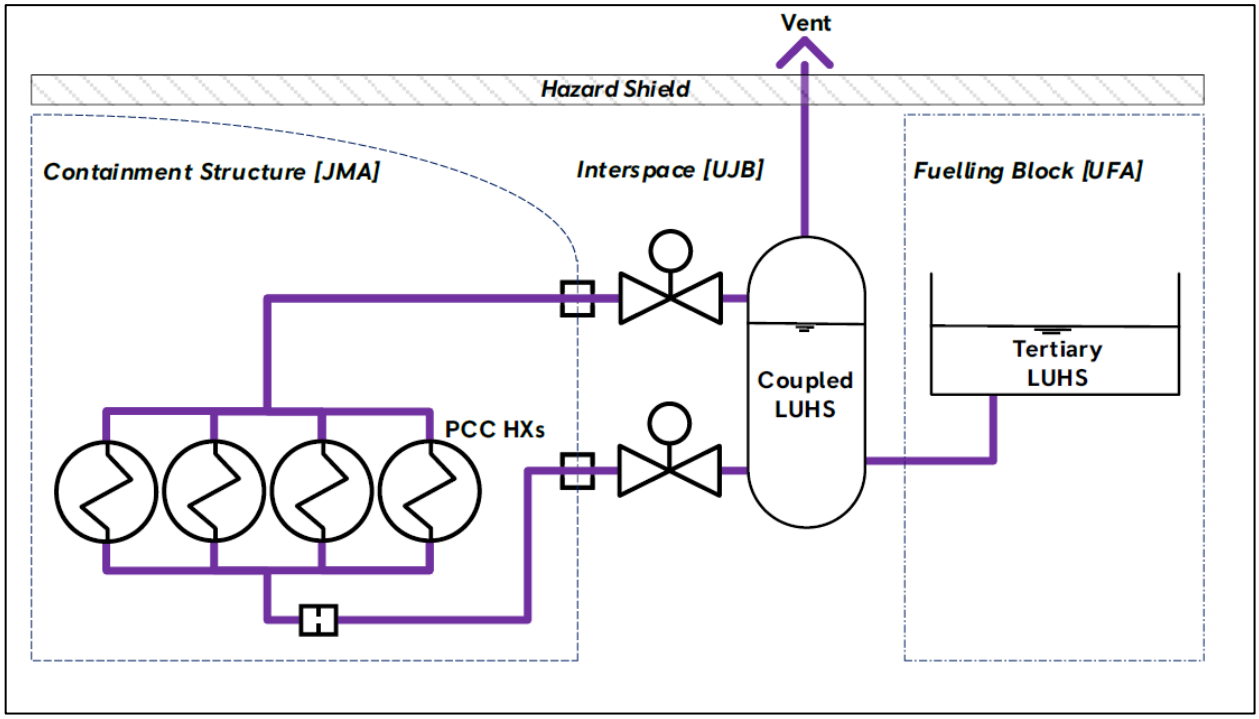


Figure 6.4-2: Simplified Schematic of Passive Containment Heat Removal

Active Containment Heat Removal

A secondary means of containment heat removal is available for severe accidents (DEC-B) using the CCSF. The CCSF can be manually aligned by the operator to enable cooling of the Containment Sump [UJA] and the containment atmosphere using the CSCS [JNA] and FPCS [FAK] cooling trains.

In recirculation mode, upon initiation of the CCSF the coolant contained in the Containment Sump [UJA] is recirculated through the FPCS [FAK] pipework and the CSCS [JNA] by the CSCS [JNA] coolant pumps, rejecting heat to CCS [KAA] using the CSCS [JNA] heat exchangers. The FPCS [FAK] pumps and heat exchangers can also be aligned to transfer heat from the Containment Sump [UJA] to the CCS [KAA]. Coolant is returned to the Containment Sump [UJA]. This heat is ultimately rejected to atmosphere through the ESWS [PBD] cooling towers.

In spray mode, the spray function allows the coolant from the Containment Sump [UJA] to be returned to containment through a spray header located in the containment upper dome. This function also uses the CSCS [JNA] coolant pumps, rejecting heat into the CCS [KAA] using the CSCS [JNA] heat exchangers. A connection to the Fire Water System (FWS) [XGB] is included to the containment spray header. Spraying coolant into the Containment [JMA] atmosphere using the FWS [XGB] transfers heat from the containment atmosphere to the coolant reducing the containment pressure. The sprayed coolant collects in the Containment Sump [UJA] where it can be recirculated as part of the CCSF.

A simplified schematic of the CCSF is illustrated in Figure 6.4-3.

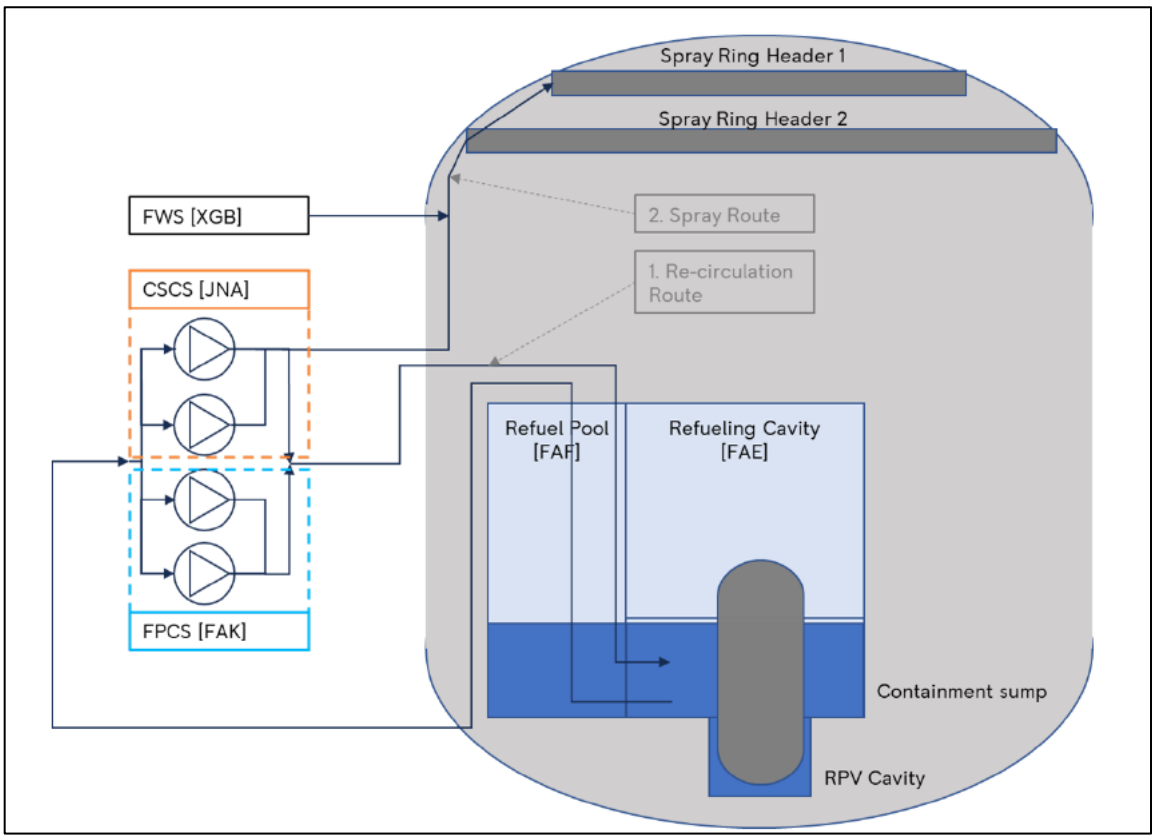


Figure 6.4-3: Simplified Schematic of Containment Cooling and Spray Function

6.4.4.4 Materials

The description and justification of materials used for Class 1 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.4.4.5 Interfaces with Supporting Systems

To support the safe operation and control, the Reactor Control and Protection System [JY] will monitor a range of key system parameters and provide indication of their level or status to the operator in the MCR and in the SCR, these parameters are described in [29].

6.4.4.6 System and Equipment Operation

As described for CSM [JM01] in section 6.4.1.6.

6.4.4.7 Instrumentation and Control

As described for CSM [JM01] in section 6.4.2.5.

6.4.4.8 Examination, Monitoring, Inspection and Testing

As described for CSM [JM01] in section 6.4.1.8

6.4.4.9 Radiological Aspects

As described for CSM [JM01] in section 6.4.1.9.

6.4.4.10 Performance and Safety Evaluation

As described for CSM [JM01] in section 6.4.1.10

6.4.5 Systems for Control of Hydrogen in Containment

6.4.5.1 System and Equipment Functions

The primary function of the HRS [JMT] is to manage hydrogen gas concentration within containment. The HRS [JMT] utilises PARs to recombine hydrogen to water, and includes hydrogen monitors to monitor hydrogen concentrations within the Containment System [JMA]. The HRS [JMT] supports the FSF of CoRM during DBCs and DECs, achieved as part of the CSM [JM01] variants 3 and 4 described in section 6.4.1.

6.4.5.2 Design Bases

The design bases for the Containment System [JMA], including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

During frequent faults (DBC-3ii and DBC-4), hydrogen mitigation has been identified as a protective function in support of the CSM [JM01] variant 3. The first protective function is provided by the containment free air volume, which ensures global concentrations remain below the lower flammability limit (4%) and is assigned a safety category A. The second protective function is provided by the PARs, which are assigned a safety category B.

During severe accidents (DEC-B), hydrogen reduction is a mitigative function that supports the CSM [JM01] variant 4, which is assigned safety category C.

Equipment required to fulfil safety category B functions are assigned a safety class 2; the HRS [JMT] includes two safety class 2 PAR units.

Equipment required to fulfil safety category C functions are assigned safety class 3; the HRS [JMT] includes 28 safety class 3 PAR units and two safety class 3 hydrogen monitors.

No environment, security, or safeguards classification is assigned at RD7/DRP1.

The seismic performance classification of PARs and hydrogen monitoring are SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.4.5.3 Description

The HRS [JMT] comprises equipment to monitor and reduce hydrogen concentrations. Hydrogen reduction is achieved through recombination of hydrogen with oxygen, utilising PARs. Key components of HRS [JMT] include the PARs and the hydrogen monitors, there is no major pipework or sub-systems included in HRS [JMT].

PARs are strategically placed throughout containment near hydrogen sources or in areas where hydrogen could accumulate. Monitors are strategically placed in areas where hydrogen could accumulate. Each PAR is positioned away from SSCs to reduce the risk of dropped load hazards. Additionally, the PARs are positioned ensuring the hot exhaust plume does not impinge on SSCs.

During both DBCs and DECs, the capacity of the relevant PARs is sized to ensure 1oo2 redundancy to deliver the safety function.

Further description of the HRS [JMT] is provided in the HRS SDD [32].

6.4.5.4 Materials

The PARs and monitors are supplied from vendors and qualified using appropriate materials to deliver their functions during DBCs and DECs.

6.4.5.5 Interfaces with Supporting Systems

The Reactor Control and Protection System [JY] provides indication of hydrogen concentrations inside containment to the operator in the MCR and the SCR.

6.4.5.6 System and Equipment Operation

In the event of a fault which requires the HRS [JMT], no operator action is required to initiate the system; the HRS [JMT] is passive and will operate when hydrogen is released into the containment atmosphere. The HRS [JMT] system will then recombine the hydrogen released to containment lowering the hydrogen concentrations within containment.

6.4.5.7 Instrumentation and Control

The Reactor Control and Protection System [JY] will monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the SCR. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits. No operator action is required to initiate or control the PARs.

6.4.5.8 Examination, Monitoring, Inspection and Testing

As described for CSM [JM01] in section 6.4.1.8

6.4.5.9 Radiological Aspects

As described for CSM [JM01] in section 6.4.1.9.

6.4.5.10 Performance and Safety Evaluation

As described for CSM [JM01] in section 6.4.1.10

6.4.6 Mechanical Features of Containment

6.4.6.1 Containment Isolation System

6.4.6.1.1 System and Equipment Functions

The function of containment isolation is to prevent the release of radioactive material to atmosphere through fluid system penetrations during DBCs and DECs. Containment isolation supports the FSF of CoRM, achieved as part of the CSM [JM01] variants 2, 3 and 4, described in section 6.4.1. It also supports delivery of the ECC [JN01], described in section 6.1.1.

6.4.6.1.2 Design Bases

The design bases for containment isolation as part of the CSM [JM01], including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

Containment isolation is demanded as part of the safety category A function delivered by the CSM [JM01] variant 3, containment isolation valves are classified as safety class 1 in accordance with the E3S categorisation and classification methodology outlined in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

No environment, security, or safeguards classification is assigned at RD7/DRP1.

The seismic performance classification of the CSM [JM01] is SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.4.6.1.3 Description

Fluid systems which pass through containment include isolation valves. Five generic types of fluid system penetrations have been defined for the different fluid system configurations expected to penetrate the Containment System [JMA] [29]:

6.4.6.1.4 Materials

The description and justification of materials used for Class 1 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.4.6.1.5 Interfaces with Supporting Systems

Containment isolation is reliant on the Reactor Control and Protection System [JY] to initiate automatically, see section 6.4.6.1.7. Containment isolations for variants 2 and variants 3 initiate automatically. CSM [JM01] variant 4, and associated subfunctions, are initiated manually from the MCR as part of the severe accident response.

6.4.6.1.6 System and Equipment Operation

Containment isolation valves are assumed to remain in their normal position if a control function is not defined as part of a fault response. As faults progress through preventative, protective and mitigating defence in depth levels, containment isolation valves ensure non-essential systems are isolated and systems supporting active safety measures are open. There are four modes of the containment isolation function, dependent on fault progression, that initiate in response to defined plant states:

1. Containment isolation mode 1 (LOCA), alignment which initiates on low pressuriser level or pressure or high containment pressure, isolates penetrations for CVCS [KBE], FPCS [FAK], Sampling {KUA, KUB, KUF], Chilled Water [KJL], CSCS [JNA] and Containment HVAC [KLA].

2. Containment isolation mode 2 (ECC Phase 1), which initiates on high HP EBD valve flow or temperature, isolates penetrations for Steam Feed [LBA, LBK], ASD Valves [LBK50], Feedwater [LAB, LCQ], CVCS [KBE], FPCS [FAK], Sampling [KUA, KUB, KUF], Chilled Water [KJL], CSCS [JNA], HPIS [JND], EBIS [JDK], PSCS [JNB], CCS [KAA] and Containment HVAC [KLA].

3. Containment isolation mode 3 (ECC Phase 2), which initiates on low accumulator level, isolates penetrations for Steam Feed [LBA, LBK], ASD Valves [LBK50], Feedwater [LAB, LCQ],

CVCS [KBE], FPCS [FAK], Sampling [KUA, KUB, KUF], Chilled Water [KJL], CSCS [JNA], HPIS [JND], EBIS [JDK], LPIS [JNG], PSCS [JNB], CCS [KAA] and Containment HVAC [KLA].

4. Containment isolation mode 4 (severe accidents), which initiates upon operator demand in response to a severe accident, isolates penetrations for Steam Feed [LBA, LBK], ASD Valves [LBK50], Feedwater [LAB, LCQ], CVCS [KBE], FPCS [FAK], Sampling [KUA, KUB, KUF], Chilled Water [KJL], HPIS [JND], EBIS [JDK], LPIS [JNG], PSCS [JNB], CCS [KAA] and HVAC [KLA]. Notably, FPCS [FAK] penetrations are not closed in this mode to permit CCSF on operator demand.

Further details of the containment isolation alignment through the fault progression are provided in [29].

6.4.6.1.7 Instrumentation and Control

The isolation of pipework penetrations through isolation valves is controlled by the Reactor Control and Protection System [JY]. During all modes of operations, the actuation of isolation valves when undertaking a confinement function is defined by the CSM [JM01], described in section 6.4.1. The CSM [JM01] defines the control logic for containment isolation valves during fault conditions including the control signal required to initiate their actuation and the valve response.

Containment Isolation for CSM [JM01] variant 3 is a safety category A function and is therefore assigned to both the RPS [JRA] and the DPS [JQ]. The Containment Isolation for CSM [JM01] variant 2 is a safety category B function and is therefore assigned to RPS [JRA].

6.4.6.1.8 Examination, Monitoring, Inspection and Testing

As described for CSM [JM01] in section 6.4.1.8

6.4.6.1.9 Radiological Aspects

As described for CSM [JM01] in section 6.4.1.9.

6.4.6.1.10 Performance and Safety Evaluation

As described for CSM [JM01] in section 6.4.1.10

6.4.6.2 Systems for Protection against Overpressure and Underpressure

6.4.6.2.1 System and Equipment Functions

The function of the severe accident depressurisation is to depressurise the RCS [JE] during DEC-B to mitigate HP melt ejection and direct containment heating that could challenge the containment integrity. Severe accident depressurisation supports the FSF of CoRM, achieved as part of the CSM [JM01] variant 4, described in section 6.4.1.

6.4.6.2.2 Design Bases

The design bases for severe accident depressurisation as part of the CSM [JM01], including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

Severe accident depressurisation is demanded as part of the safety category C function delivered by the CSM [JM01] variant 4. It is however noted that components delivering the depressurisation function also deliver overpressure protection functions that are safety category A (see section 6.1.1) and therefore are classified as safety class 1 in accordance with the E3S categorisation and classification methodology outlined in E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2].

No environment, security, or safeguards classification is assigned at RD7/DRP1.

The seismic performance classification of the CSM [JM01] is SPC1 in accordance with E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.4.6.2.3 Description

There are two methods available to depressurise the RCS [JE] during DEC-B accidents:

1. Manual depressurisation using the Reactor Coolant Pressure Relief System [JEG] HTOP safety relief valves (SRVs)

2. Manual depressurisation using the Automatic Isolation Valves (AIVs) on the LP ADS [JNF]

The Reactor Coolant Pressure Relief System [JEG] has two HTOP trains, each with a single SRV. The SRVs discharge into the Refuelling Pool [FAF] through spargers. Spurious C&I actuation is prevented by electrically isolating the motor pilot operated valves.

The ADS [JNF] has three LP trains, each with a single AIV. If the RCS pressure has exceeded relevant limits, the EBD valve in series with each AIV will open. Spurious actuation of the LP ADS lines is prevented by the EBD valve design.

A simplified schematic of the severe accident depressurisation system is illustrated in Figure 6.4-4. Further details of the Reactor Coolant Pressure Relief System [JEG] are provided in E3S Case Version 2, Tier 1, Chapter 5: Reactor Coolant System and Associated Systems [18].

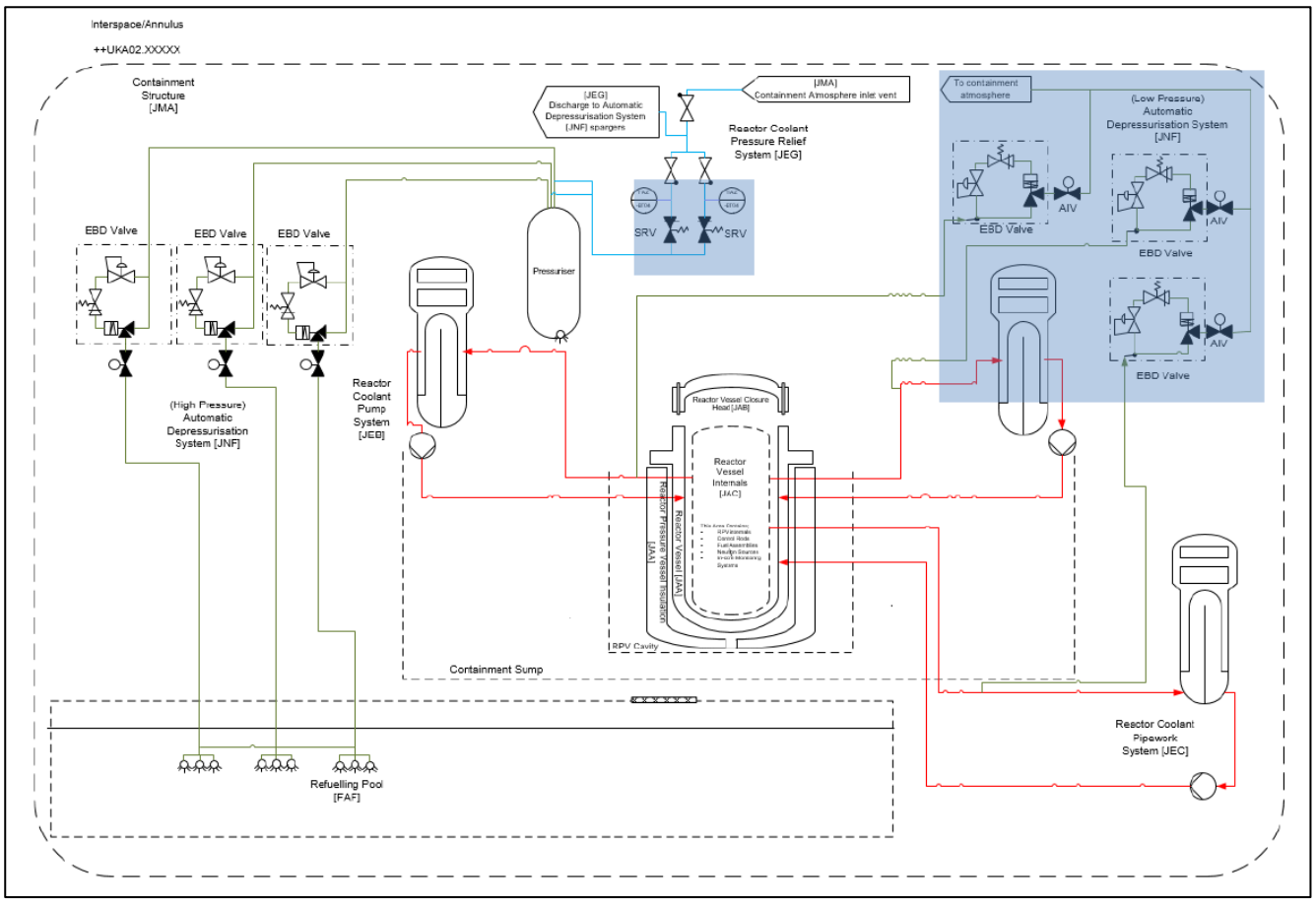


Figure 6.4-4: Simplified Schematic of Severe Accident Depressurisation (highlighted blue)

6.4.6.2.4 Materials

The description and justification of materials used for Class 1 SSCs are presented in E3S Case Version 2, Tier 1, Chapter 23: Structural Integrity [1].

6.4.6.2.5 Interfaces with Supporting Systems

Severe accident depressurisation is reliant on the Reactor Control and Protection System [JY], see section 6.4.6.2.7.

6.4.6.2.6 System and Equipment Operation

In response to high core exit temperature, the operator can manually initiate opening of the motor operated pilot valves which open the HTOP SRVs [JEG]. The valve will be electrically isolated in normal operations, so the operators first action will be to de-isolate the valve prior to initiating any systems. All of the HTOP SRVs [JEG] will open on demand.

If the HTOP SRVs [JEG] fail to operate, the operator will manually initiate opening of the LP ADS AIVs [JNF]. The LP ADS AIVs [JNF] will open on demand if not already open. The LP ADS EBD valves [JNF] open automatically.

6.4.6.2.7 Instrumentation and Control

The severe accident depressurisation function as part of CSM [JM01] variant 4 is assigned to the SAMS [JRQ20].

6.4.6.2.8 Examination, Monitoring, Inspection and Testing

As described for CSM [JM01] in section 6.4.1.8

6.4.6.2.9 Radiological Aspects

As described for CSM [JM01] in section 6.4.1.9.

6.4.6.2.10 Performance and Safety Evaluation

As described for CSM [JM01] in section 6.4.1.10

6.4.6.3 Penetrations

The Pipework Penetration Assemblies [PT260] and Electrical Penetration Assemblies [PT270] are part of the Containment System [JMA], described in section 6.4.2. Containment isolation valves that isolate the flow of fluid through the penetrations are described in section 6.4.6.1.

6.4.6.4 Airlocks, Doors, and Hatches

The Main Equipment Access Hatch [PT251] and Personnel Airlock [PT252] are part of the Containment System [JMA], described in section 6.4.2.

6.4.7 Heading Section Not Used

This section is reserved for designs with an annulus around containment in the IAEA safety report format [31] and is not used by RR SMR.

6.4.8 Ventilation System

6.4.8.1 System and Equipment Functions

The principal function of the Containment HVAC [KLA] is to provide heating, ventilation, and air conditioning to the primary Containment System [JMA] and reduce airborne activity. It supports the FSF of CoRM, achieved as part of the CSM [JM01] variant 1, described in section 6.4.1.

6.4.8.2 Design Bases

The design bases for Containment HVAC [KLA] as part of the CSM [JM01], including associated E3S categorised functional requirements and non-functional system requirements, are presented in section 6.4.1.

The Containment HVAC [KLA] supports the safety category C function to reduce airborne activity during normal operation. These functions are delivered by safety class 3 SSCs in accordance with the E3S categorisation and classification methodology outlined in E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2].

No environment, security, or safeguards classification is assigned at RD7/DRP1.

The seismic performance classification of the CSM [JM01] is SPC1 in accordance with E3S Case Chapter 3: E3S Objectives and Design Rules for SSCs [2].

6.4.8.3 Description

The Containment HVAC [KLA] consists of a ventilation system, a containment air cleaning system, and a containment cooling system. The ventilation system supplies fresh air from two air handling units. The exhaust system exhausts containment air via high efficiency particulate air (HEPA) filters. The air cleaning system scrubs iodine from the containment air.

Containment HVAC [KLA] ventilation is provided by two supply air handling units in parallel. Containment HVAC [KLA] exhaust is provided by two exhaust fans in parallel and two HEPA filter banks in parallel. Exhaust is discharged from the building via the Stack [KLS]. Containment HVAC [KLA] air cleaning is provided by two iodine filtration lines in parallel. Containment HVAC [KLA] cooling is provided by five cooling coil units in parallel.

Single extract ductwork network extracts air from primary containment via extract air grilles and routes it back to the main primary containment extract plant. Safety Class 1 isolation valves are in the extract ductwork as it penetrates the hazard shield and primary containment to enable isolation of the system from the space and maintain the physical integrity of the containment barrier in the event of an accident.

Further details of the Containment HVAC [KLA] are provided in the HVAC SDD [33].

6.4.8.4 Materials

The description and justification of materials used for safety classified SSCs are presented in E3S Case Chapter 23: Structural Integrity [1].

6.4.8.5 Interfaces with Supporting Systems

The Containment HVAC [KLA] is a supporting system to the primary Containment System [JMA].

The Containment HVAC [KLA] interfaces with C&I systems to provide monitoring and alarms.

6.4.8.6 System and Equipment Operation

The HVAC systems operate to maintain an air flow from the areas of lower levels of airborne contamination to those with higher levels of airborne contamination to prevent the spread through the building and release of contamination to the atmosphere. The Containment HVAC [KLA] recirculating filtration system will operate automatically as required based on airborne contamination levels within primary containment.

6.4.8.7 Instrumentation and Control

The Reactor Island and Protection System [JY] will monitor a range of key systems parameters and provide indication of these to the operator in the MCR and in the SCR. It will also provide alarms to indicate that key system parameters are outside of the defined performance bands and/or safety limits, with details provided in [33].

6.4.8.8 Examination, Monitoring, Inspection and Testing

As described for CSM [JM01] in section 6.4.1.8.

6.4.8.9 Radiological Aspects

The HVAC systems maintain an air flow from the areas of lower levels of airborne contamination to those with higher levels of airborne contamination to prevent the spread through the building and release of contamination to the atmosphere.

6.4.8.10 Performance and Safety Evaluation

As described for CSM [JM01] in section 6.4.1.10.

6.4.9 Filtered Venting System

The design of the RR SMR does not incorporate a filtered venting system.

6.4.10 Containment Leakage System

Containment leakage is managed and minimised through the design of the steel Containment Vessel Structure [PT250] and associated penetrations, described in section 6.4.2. Containment leak rate testing for CSM [JM01] is described in section 6.4.1.8.

6.5 Habitability Systems

The habitability systems for the RR SMR include the MCR, SCR, and emergency response facilities including the emergency response centre (ERC), technical support centre (TSC) and operational support centre (OSC). It will also include multiple security facilities and arrangements for an offsite emergency response centre. These are described further in E3S Case Version 2, Tier 1, Chapter 19: Emergency Preparedness and Response [34].

6.6 Systems for Removal and Control of Fission Products

The principal function of the containment airborne radioactive material reduction function is to reduce the inventory of radioactive material in the containment atmosphere during normal operation and faulted conditions.

The RR SMR includes the several features to minimise the inventory of mobile fission products:

- Containment HVAC [KLA] which includes an air cleaning function during normal operation, described in section 6.4.8
- Natural phenomena (NC, condensation, and deposition on containment and its internal components) within the Containment System [JMA], described in section 6.4.2
- Intermittent spray function by CCSF (during DEC-B conditions), described in section 6.4.4

Decisions on further measures for pH control will be reported in Version 3 of the E3S Case.

6.7 Conclusions

6.7.1 ALARP, BAT, Secure by Design, Safeguards by Design

The design of all SSCs presented in this chapter are developed in accordance with the systems engineering design process. This 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 criteria that ensure risks are reduced to ALARP, apply BAT, and are secure by design and safeguards by design, as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [2]. This provides confidence that claims can be met when the full suite of arguments and evidence is developed.

A summary of key design decisions made with respect to ensuring overall risks are reduced to ALARP, BAT, secure by design and safeguards by design for each safety measure is provided in respective sections of this chapter, based on design decisions up to RD7/DRP1. The overall demonstration of ALARP, BAT, secure by design and safeguards by design at RD7/DRP1 is presented in E3S Case Version 2, Tier 1, Chapters 24, 27, 32 and 33 respectively.

6.7.2 Assumptions and Commitments on Future Dutyholder / Licensee / Permit Holder

None identified in this revision.

6.7.3 Conclusions and Forward Look

The generic E3S Case objective at Version 2 is 'to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design' [4]. This confidence is built through development and underpinning of top-level claims across each chapter of the E3S Case, through supporting arguments and evidence. The top-level claim for chapter 6 is "*Engineered Safety Features are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with secure-by-design and safeguards-by-design*".

The arguments and evidence presented to meet the generic E3S Case objective at Version 2 include the selection of appropriate codes and standards that follow RGP. Safety functions are identified aligned to the FSFs, which are categorised in accordance with the E3S categorisation and classification methodology, with SSCs assigned both a safety and seismic classification.

The design and layout of SSCs at RD7/DRP1 are also developed and evaluated in accordance with the E3S design principles through the integrated E3S and engineering processes [2], including design optioneering, to drive risk reduction to ALARP, and to demonstrate BAT, secure by design and safeguards by design. For example, the safety class 1 ECC [JN01] measure is designed with three redundant trains to ensure its safety function can be delivered in the presence of a single failure, each of which are segregated to minimise the loss of multiple trains due to an internal hazard such as fire. Environment, security, and safeguards aspects are also considered, for example, ASF [JD02] is designed with boron mixing in the Refuelling Pool [FAF], which reduces the volume of solid and borated waste over the lifetime of the plant. This provides confidence that E3S functions can be achieved by the design as functional requirements are derived through ongoing and iterative E3S analyses.

Further arguments and evidence to underpin the claim will be developed in line with the E3S Case Route Map [5] and reported in future revisions of the generic E3S Case, which will further build confidence that the RR SMR can deliver its fundamental E3S objective. This broadly includes continued iterative E3S analysis and finalisation of E3S requirements including environment, security and safeguards, detailed design development of all SSCs, and V&V of E3S requirements.

6.8 References

[1] Rolls-Royce SMR Limited, SMR0004363 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 23: Structural Integrity,” May 2024.

[2] Rolls-Royce SMR Limited, SMR0004589 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs,” May 2024.

[3] Rolls-Royce SMR Limited, SMR0003977 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 15: Safety Analysis,” May 2024.

[4] Rolls-Royce SMR limited, SMR0004924 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction,” May 2024.

[5] Rolls-Royce SMR Limited, SMR0002155/003, “E3S Case Route Map,” November 2023.

[6] Rolls-Royce SMR, SMR0001603/001, “Environment, Safety, Security and Safeguards Design Principles,” August 2022.

[7] Rolls-Royce SMR Limited, SMR0000213 Issue 2, “Requirements Specification for Emergency Core Cooling [JN01],” October 2023.

[8] Rolls-Royce SMR Limited, SMR0000942 Issue 2, “Allocated Requirements from Emergency Core Cooling [JN01],” October 2023.

[9] Rolls-Royce SMR Limited, SMR0000911 Issue 2, “Safety Measure Design Description for the Emergency Core Cooling System [JN01],” October 2023.

[10] Rolls-Royce SMR Limited, SMR0003880 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 10: Steam and Power Conversion Systems,” May 2024.

[11] Rolls-Royce SMR Limited, SMR0007298 Issue 2, “Reactor Island Architectural and Layout Summary Report,” January 2024.

[12] Rolls-Royce SMR Limited, SMR0004010 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 8: Electrical Power,” May 2024.

[13] Rolls-Royce SMR Limited, SMR0006900 Isue 1, “Reactor Island Operating Philosophy,” July 2023.

[14] Rolls-Royce SMR Limited, SMR0004247 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 13: Conduct of Operations,” May 2024.

[15] Rolls-Royce SMR Limited, SMR0003939 Issue 3, “Environment, Safety, Security and Safeguards Case Vesion 2, Tier 1, Chapter 7: Instrumentation & Control,” May 2024.

[16] Rolls-Royce SMR Limited, SMR0000605 Issue 3, “Requirements Specification for Passive Decay Heat Removal [JN02],” October 2023.

[17] Rolls-Royce SMR Limited, SMR0000625 Issue 3, “Allocated Requirements from Passive Decay Heat Removal [JN02],” Octoer 2023.

[18] Rolls-Royce SMR Limited, SMR0003984 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 5: Reactor Coolant System and Associated Systems,” May 2024.

[19] Rolls-Royce SMR Limited, SMR0000624 Issue 3, “Safety Measure Design Description for Passive Decay Heat Removal [JN02],” October 2023.

[20] Rolls-Royce SMR Limited, SMR0000749 Issue 2, “Requirements Specification for the Scram [JD01] Safety Measure,” October 2023.

[21] Rolls-Royce SMR Limited, SMR0000750 Issue 2, “Allocated Requirements Specification for the Scram Function [JD01],” October 2023.

[22] Rolls-Royce SMR Limited, SMR0000639 Issue 2, “Scram [JD01] Safety Measure Design Description,” October 2023.

[23] Rolls-Royce SMR Limited, SMR0000751 Issue 2, “Requirements Specification for the Alternative Shutdown Function [JD02],” December 2023.

[24] Rolls-Royce SMR Limited, SMR0000752 Issue 2, “Allocated Requirements Specification for the Alternative Shutdown Function [JD02],” December 2023.

[25] Rolls-Royce SMR Limited, SMR0000638 Issue 2, “Safety Measure Design Description for the Alternative Shutdown Function [JD02],” December 2023.

[26] Rolls-Royce SMR Limited, SMR0005922 Issue 2, “System Description for the In-Vessel Retention Function and Reactor Cavity Injection [JNM],” December 2023.

[27] Rolls-Royce SMR Limited, SMR0004993 Issue 2, “JM01-R: Requirements Specification for the Containment Safety,” November 2023.

[28] Rolls-Royce SMR Limited, SMR0006966 Issue 1, “Allocated Requirements (D-Module) Specification for the Containment Measure [JM01],” July 2023.

[29] Rolls-Royce SMR Limited, SMR0008536 Issue 1, “Safety Measure Design Description for the Containment [JM01] Safety Measure,” November 2023.

[30] Rolls-Royce SMR Limited, SMR0005089 Issue 1, “Containment [JMA] System Design Description,” October 2023.

[31] International Atomic Energy Agency, “Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide SSG-61,” 2021.

[32] Rolls-Royce SMR Limited, SMR0006184 Issue 1, “HRS [JMT] System Design Description,” July 2023.

[33] Rolls-Royce SMR Limited, SMR0004702 Issue 1, “System Design Description for the HVAC Systems Serving Controlled Areas and Uncontrolled Areas of Reactor Island (KL),” June 2023.

[34] Rolls-Royce SMR Limited, SMR0004571 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 19: Emergency Preparedness and Response,” May 2024.

6.9 Appendix A: Claims, Arguments, Evidence

Table 6.9-1 provides a mapping of the claims to the corresponding sections of the chapter that summarise the arguments and/or evidence. The full decomposition of claims and link to underpinning Tier 2 and Tier 3 information containing the detailed arguments and evidence is presented in the E3S Case Route Map [5]. The route map includes the trajectory of Tier 2 and Tier 3 information as the generic E3S Case develops, which will be incorporated into Tier 1 chapters as it becomes available and in line with generic E3S Case issues described in [4].

Table 6.9-1: Mapping of Claims to Chapter Sections

Claim	**Section of Chapter 6 containing arguments / evidence summary**
ECC [JN01] non-functional system requirements are complete	6.1.1.2.2
ECC [JN01] non-functional system requirements are correctly assigned	6.1.1.2.2
ECC [JN01] codes and standards are correctly assigned	6.0.4
Safety requirements for the ECC [JN01] are complete	6.1.1.2.1
Environmental functional requirements for the ECC [JN01] are complete	None at this revision
Security functional requirements for the ECC [JN01] are complete	None at this revision
Safeguards functional requirements for the ECC [JN01] are complete	None at this revision
The ECC [JN01] is classified correctly	6.1.1.2.3
The ECC [JN01] design achieves its E3S functional requirements	6.1.1.3 - 6.1.1.9
The ECC [JN01] design achieves its E3S non-functional system requirements	6.1.1.3 - 6.1.1.9
The layout design facilitates the system achieving its E3S requirements	6.1.1.3
Structural integrity is substantiated commensurate with the SSC classification	Covered in E3S Case Chapter 23
The ECC [JN01] design definition is verified to meet its requirements	6.1.1.10
The implemented ECC [JN01] system is validated to meet its E3S functions	Not covered in this revision
Verification of the ECC [JN01] system is preserved through its operational life	Not covered in this revision

Claim	**Section of Chapter 6 containing arguments / evidence summary**
PDHR [JN02] *claims structure as per ECC [JN01] structure*	6.1.2
Scram [JD01] *claims structure as per ECC [JN01] structure*	6.2.1
ASF [JD02] *claims structure as per ECC [JN01] structure*	6.2.2
CSM [JM01] *claims structure as per ECC [JN01] structure*	6.3, 6.4

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	6.2.1
JD02	Alternative Shutdown Function	6.2.2
JDK	Emergency Boron Injection System	
JM01	Containment Safety Measure	6.3 and 6.4
JNM	Reactor Vessel Cavity Injection System	6.3
JMA	Containment System	6.4.1 and 6.4.2
PT250	Containment Vessel Structure	
PT253	Fuel Transfer Channel	
PT251	Main Equipment Access Hatch	
PT252	Personnel airlock	
PT260	Containment Mechanical Penetrations	
PT270	Electrical Penetrations	
JMT	Hydrogen reduction	6.4.1 and 6.4.5
KLA	Containment HVAC	6.4.8
JN01	Emergency Core Cooling System	6.1.1
JNF	Automatic Depressurisation System	
JNG	Low Pressure Injection System	
JN02	Passive Decay Heat Removal System	6.1.2
JNB	Passive Steam Condensing System	

RDS-PP®	SSC	Section in Chapter 6
JND	High Pressure Injection System	
JNK	Local Ultimate Heat Sink	6.1.1 and 6.1.2
LBK50	Atmospheric Steam Dump	6.1.2
JN03	High Temperature Heat Removal	6.1.3
JN04	Low Temperature Decay Heat Removal	6.1.4

6.11 Abbreviations

1oo'X'	One out of 'X'
ADS	Automatic Depressurisation System
AIV	Automatic Isolation Valve
ALARP	As Low as Reasonably Practicable
ASF	Alternative Shutdown Function
ASME	American Society of Mechanical Engineers
BAT	Best Available Techniques
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CCF	Common Cause Failure
CCS	Component Cooling System
CCSF	Containment Cooling and Spray Function
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRE	Control of Radiation Exposure
CoRM	Confinement of Radioactive Material
CRDM	Control Rod Drive Mechanism
CSCS	Cold Shutdown Cooling System
CVCS	Chemical and Volume Control System
CZP	Cold Zero Power
DBC	Design Basis Condition
DCH	Direct Containment Heating
DEC	Design Extension Condition
DPS	Diverse Protection System
DRP	Design Reference Point
DVI	Direct Vessel Injection

E3S	Environment, Safety, Security and Safeguards
EBD	Emergency Blow Down
EBIS	Emergency Boron Injection System
ECC	Emergency Core Cooling
EMIT	Examination, Maintenance, Inspection and Testing
EPRI	Electrical Power Research Institute
ERC	Emergency Response Centre
ESWS	Essential Service Water System
EUR	European Utility Requirements
FPCS	Fuel Pool Cooling System
FSF	Fundamental Safety Function
FWS	Fire Water System
GDA	Generic Design Assessment
HEPA	High Efficiency Air Particulate
HLSF	High-Level Safety Function
HP	High Pressure
HPIS	High Pressure Injection System
HPME	High Pressure Melt Ejection
HRS	Hydrogen Reduction System
HTHR	High Temperature Heat Removal
HTOP	High Temperature Overpressure Protection
HVAC	Heating, Ventilation, Air Conditioning
IAEA	International Atomic Energy Agency
IB	Intermediate Break
ICF	Intact Circuit Fault
IHP	Integrated Head Package
ILRT	Integrated Leak Rate Test
ISI	In-Service Inspection
IVR	In-Vessel Retention

LB	Large Break
LLRT	Local Leak Rate Test
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LP	Low Pressure
LPIS	Low Pressure Injection System
LUHS	Local Ultimate Heatsink System
LVCS	Level and Volume Control System
MCCI	Molten Core-Concrete Interaction
MCR	Main Control Room
MSCV	Multi-Stage Control Valve
MSLB	Main Steam Line Break
MSIV	Main Steam Isolation Valve
NC	Natural Circulation
NOP	Normal Operating Pressure
NOT	Normal Operating Temperature
OPEX	Operating Experience
OSC	Operational Support Centre
PAMS	Post-Accident Management System
PAR	Passive Autocatalytic Recombiners
PCC	Passive Containment Cooling
PDHR	Passive Decay Heat Removal
PFD	Probability of Failure on Demand
PIE	Postulated Initiating Event
PMBD	Preventative Maintenance Basis Database
PSCS	Passive Steam Condensing System
PWR	Pressurised Water Reactor

RCM	Reliability Centred Maintenance
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RD	Reference Design
RDS-PP	Reference Designation System for Power Plants
RGP	Relevant Good Practice
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RR SMR	Rolls-Royce Small Modular Reactor
RVCIS	Reactor Vessel Cavity Injection System
SAMG	Severe Accident Management Guidelines
SAMS	Severe Accident Management System
SBO	Station Blackout
SCR	Supplementary Control Room
SDD	System Design Description
SDM	Shutdown Margin
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SMDD	Safety Measure Design Description
SPC	Seismic Performance Class
SRV	Safety Relief Valve
SSC	Structure, System, and Component
TLA	Through-Life Activity
TSC	Technical Support Centre
UK	United Kingdom
V&V	Verification & Validation