Partner Document Number	Partner Document Issue /Revision	Retention Category
n/a	n/a	A

Title

E3S Case Chapter 24: ALARP Summary

Executive Summary

This chapter of the Environment, Safety, Security, and Safeguards (E3S) Case presents the As Low As Reasonably Practicable (ALARP) summary for the Rolls-Royce Small Modular Reactor (RR SMR). The chapter outlines the arguments and preliminary evidence available at the Preliminary Concept Definition (PCD) design stage to underpin the high-level Claim that the design of the RR SMR reduces nuclear and conventional safety risks to ALARP through the lifecycle.

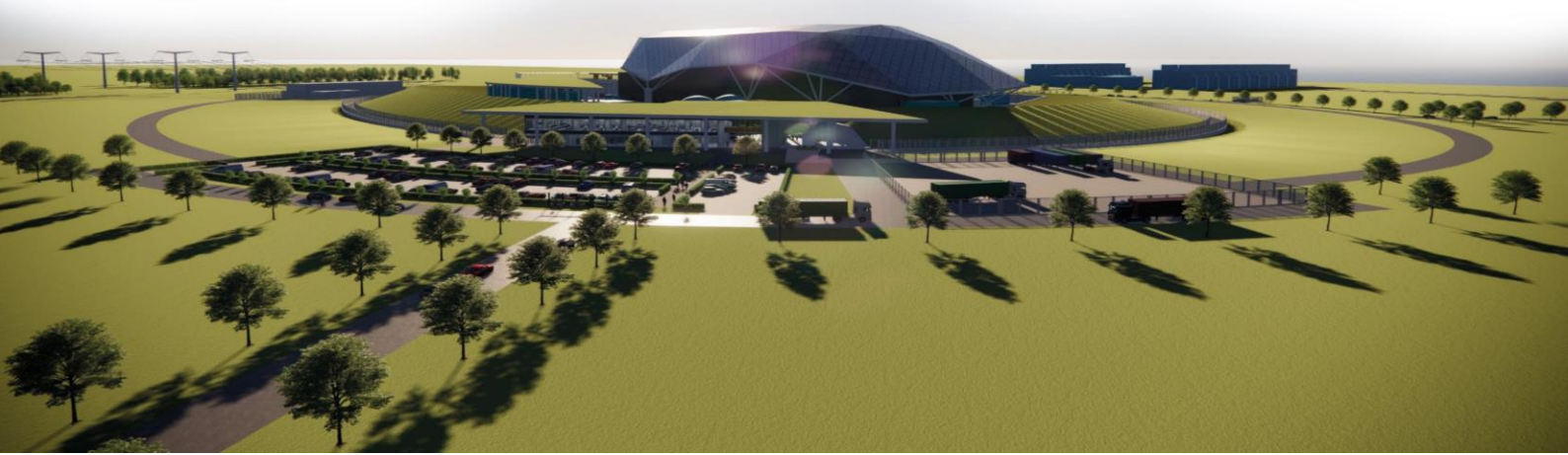
The RR SMR design utilises E3S techniques (including the hierarchy of controls, deterministic and probabilistic analysis) to ensure the risk of any hazard, including exposure to radioactive materials, is reduced to ALARP.

E3S techniques have informed the RR SMR design, including:

1. Design Decisions – to ensure compliance with E3S principles
2. Layout – to protect against internal hazards and to integrate human factors
3. Systems – to ensure they are passive, redundant, diverse and segregated, with multiple means of removing decay heat in response to faults
4. Structures (e.g., hazard shield and aseismic bearing) – to protect Structures, Systems and Components (SSCs) from external hazards

This chapter summarises evidence from across the E3S Case, available at the PCD stage, and describes how ALARP principles are being embedded early into the design process, leading to outputs that support risk reduction to ALARP.

The evidence at PCD supports the position that RR SMR risks can be reduced to ALARP, noting further evidence to support the Claim and overall ALARP demonstration is being developed through the ongoing design programme.



Contents

Tables

24.1 Introduction

24.1.1 Introduction to Chapter

Chapter 24 of the Rolls-Royce Small Modular Reactor (RR SMR) Environment, Safety, Security and Safeguards (E3S) Case forms part of the Pre-Construction Safety Report (PCSR), as defined in E3S Case Chapter 1: Introduction, Reference [1].

Chapter 24 presents the overarching summary of how the RR SMR reduces risk to As Low As Reasonably Practicable (ALARP) based on the design and safety information presented across the E3S chapters, as defined at Reference Design (RD) 5 level of design maturity.

As this is an ALARP summary chapter from across the E3S Case, this chapter references other E3S Chapters, and where further/background information is deemed useful, additional Tier 3 evidence is referenced (e.g., decision files etc.). An interim ALARP Summary Report (Tier 2 evidence) will be made available in a future revision of the E3S Case (refer to Section 24.1.4).

24.1.2 Background to ALARP

The term ALARP arises from Great Britain's (GB) legislation, which requires provision and maintenance of plant and systems of work that are, 'so far as is reasonably practicable', safe and without risks to health.

So Far As Is Reasonably Practicable (SFAIRP) is interpreted as leading to a legal requirement that risks must be reduced to a level that is ALARP; these principles apply to the demonstration of the application of Best Available Techniques (BAT), as part of compliance with Environmental Law.

In determining whether a risk is ALARP, the definition of Reasonably Practicable is key, in that the risk must be significant in relation to the sacrifice (in terms of time, trouble and cost) required to avert it. Risks must be averted unless there is a gross disproportion between costs and benefits of doing so; this concept of gross disproportion means that an ALARP judgement in GB is not a simple cost benefit analysis but is weighted to favour carrying out safety improvements.

The method for demonstrating that risks have been reduced to a level that is ALARP applies to all stages of the lifecycle of RR SMR and should be proportionate to the level of risk presented.

Rolls-Royce SMR ALARP principles are described in the E3S Design Principles document, Reference [2].

It is worth noting ALARP is used in GB whereas As Low As Reasonably Achievable (ALARA) is a widely recognised acronym by worldwide organisations; such as, International Atomic Energy Agency (IAEA), Nuclear Regulatory Commission (NRC), World Nuclear Association (WNA) etc. ALARA and ALARP are equivalent in meaning and purpose, Reference [3].

24.1.3 Scope

The scope of this report covers all aspects of the PCSR, covering nuclear and conventional safety, providing a holistic summary of the evidence presented within each chapter.

The scope covers the Rolls-Royce SMR ALARP process, as well a summary of the outputs from the process to demonstrate that the principle of ALARP is embedded within the RR SMR design and to determine whether further reasonable, practicable improvements could be implemented to further reduce the risks as the design develops.

Design/Programme Maturity

The ALARP position presented in this revision of the PCSR is based on the design definition and E3S analysis undertaken at the end of the Preliminary Concept Definition (PCD) design stage, which will continue to evolve alongside the ongoing design development and analysis.

An interim statement on ALARP will be presented in the ALARP Summary Report that will be presented in a future revision of the E3S Case (refer to Section 24.1.4).

24.1.4 Claims, Arguments, Evidence Route Map

The Chapter level Claim for E3S Case Chapter 24: ALARP Summary is:

Claim 24: The design of the RR SMR reduces nuclear and conventional safety risks to As Low As Reasonably Practicable through the lifecycle

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

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

24.1.5 Applicable Regulations, Codes and Standards

The following references provide key guidance and Relevant Good Practice (RGP) for ALARP:

1. Health and Safety Executive, Health and Safety at Work Act, Reference [5]

2. Office for Nuclear Regulation (ONR), Safety Assessment Principles (SAPs), includes numerical targets and safety limits: Basic Safety Objectives (BSO) and Basic Safety Limits (BSLs), Reference [6]

3. Health and Safety Executive, Reducing Risks, Protecting People (R2P2) provides guidance on the process of decision making, including risk assessment and risk management, Reference [7]

4. International Atomic Energy Agency, Fundamental Safety Principles, Reference [8]

5. Western European Nuclear Regulators Association (WENRA), Safety Reference Levels for Existing Reactors, Reference [9]

6. Health and Safety Executive, Ionising Radiation Regulations, Reference [10]

7. The Application of ALARP to Radiological Risk, Reference [3]

24.2 ALARP in Decision Making Process

24.2.1 Process & Methodology

For the RR SMR design, guidance on ALARP principles (collated mainly from the RGP and guidance outlined in Section 24.1.5) is captured in the E3S Principles document, see Reference [2]; these principles are embedded in the Conduct Design Optioneering Process C3.2.2-2 and associated Design Decision Record template used to capture design decision making [11].

This process includes the 20 key design objectives and criteria against which the design options are evaluated. Design decisions are recorded, and the Design Optioneering process is continuously reviewed and updated.

Although the decision record template has been refined over a few iterations to improve its useability, its fundamental structure and approach has not changed. The process has always included evaluation against the 20 key design objectives and criteria which include business and E3S topics, with weightings agreed at project level to ensure consistency.

Predefined weightings associated with each of the criteria have been generated based on an Analytical Hierarchical Process (AHP) to provide a clear three tier weighting of the assessment criteria; this approach provides a consistent measure for design decisions that ensures business strategic objectives are met.

The criteria, and associated weightings, have been agreed by the Chief Engineer, Chief Plant Engineer and Head of Engineering Integration, supported by Chief Design Engineers and other key stakeholders including E3S and Business Development. For more information, see Reference [12].

A comprehensive review of RGP and Operating Experience (OPEX) has formed part of all RR SMR optioneering studies, collated in a design decision template (presented in Reference [11]) that marshals the presentation of this information together to present the arguments and evidence in support of decisions reducing risk to ALARP. The information documented includes:

1. Detailed descriptions for scoring the impact of the decision on nuclear and conventional safety, environment, security and safeguards (the impact of the decision determines the type of assessment required)

2. Identification of Relevant Good Practice (RGP) and OPEX to support identification of design options

3. Development of design options and exclusions through functional means analysis, options feasibility assessment and coarse screening (e.g., advantages vs disadvantages)

4. An evaluation of the impact of design options against:

    a. Compliance with Safety Functional Requirements (SFRs) and non-functional system requirements

    b. RGP and OPEX

c. Postulated Initiating Events (PIEs) and faults or hazards, including potential to add or remove PIEs, increase or decrease their magnitude, increase or decrease Initiating Event Frequencies (IEFs), or increase or decrease the magnitude or effects/consequences of faults or hazards

d. Provision of DiD and the number or independence of available measures in the Fault Schedule (prevention, protection or mitigation)

e. Categorisation and Classification

f. Probabilistic Safety Analysis (PSA) with a comparison against numerical targets

g. Radiological aspects highlighting the benefit and detriment in relation to the hierarchy to fulfil the statutory requirements of Ionising Radiations Regulations (IRR17)

h. Criticality safety and conventional health and safety

i. Environmental impacts, including radiological environmental aspects, waste hierarchy and sustainability

j. Security impacts, including vulnerability assessments

k. Human Factors (HF) impacts

This information is used to support a decision analysis in accordance with a proportionate level of detail (as per bullet point 1), undertaken as part of a multi-disciplinary review with E3S as key stakeholders, resulting in down-selection of the design solution(s).

All design decisions are documented in the RR SMR Decision Register, Reference [13]. The register captures the following data:

1. A unique ID for the decision
2. The decision level
3. A summary of the outcome
4. Brief summary of options considered
5. The rationale behind the outcome
6. Identification as to whether the item is nuclear safety related
7. The owner of the decision
8. Status of the decision

24.2.2 Optimisation of ALARP with BAT and Secure-by-Design

Processes to ensure holistic optimisation of the RR SMR design with respect to ALARP, BAT and Secure-by-Design, have been developed to inform the RR SMR design development programme, ranging from management arrangements to front-end engineering design development processes, summarised below.

Amalgamation of Environment, Safety, Security and Safeguards Disciplines

A key enabler for the holistic approach to optimisation is the amalgamation of the RR SMR E3S functions into a single team (the E3S team) under the leadership of a Head of E3S Case to facilitate a joined-up approach to design optimisation, ensuring that potentially conflicting E3S objectives are identified and resolved early on during the optioneering stage.

An engineering interface team facilitates the engagement between the E3S team and design engineering teams, and to coordinate the integration of E3S requirements into the design development.

Further details of the management arrangements for E3S are described in E3S Case Chapter 17: Management of E3S and Quality Assurance, Reference [14].

Integrated decision process

The RR SMR design decision process (outlined in Section 24.2.1 and documented in Reference [11]) includes a structured decision analysis process that is proportionate to the overall complexity and significance of decisions (e.g., in terms of E3S, cost or project objectives and constraints) for evaluating design options and selection of preferred solution. The decision analysis (optioneering) process comprises the following three-tiers:

1. A simple comparison of relative advantages and disadvantages of options for low significance and complexity decisions

2. The use of Red-Amber-Green (RAG) qualitative evaluation scheme for decisions with moderate significance and complexity

3. Semi-quantitative analysis using the Pugh matrix for decisions with high significance and complexity

This structured tiered approach ensures consistency is applied to decision making and that the scrutiny of options is proportionate to the complexity and significance of decisions.

The decision analysis at each tier requires the evaluation of E3S factors, including ALARP, BAT, security, and safeguards considerations, alongside project factors such as cost, programme, and market demands. This review is undertaken by a multi-disciplinary team involving key stakeholders from the E3S team.

24.3ALARP in Design Development

24.3.1 Plant Level Design Development

The following section provides a brief overview of key design decisions (up to PCD design stage) for the wider plant level, to provide context to the current optioneering phase of the project and the on-going design development of the RR SMR.

Reactor Type

The selection of Pressurised Water Reactor (PWR) technology over other reactor types (e.g., Boiling Water Reactor (BWR) or Molten Salt Reactor etc.) was due to its proven technology, optimum power density and the right technology for Rolls-Royce SMR to develop, given the vast amount of OPEX in designing, manufacturing, installing, testing, commissioning, maintaining and refurbishing PWRs.

Reactor Coolant System

Design options considered a two, three and four loop Reactor Coolant System (RCS) configuration. The optimised plant layout selected is a 3-loop RCS configuration, which minimises the footprint of the Reactor Island for the compact layout. For more information, see Reference [15].

Decay Heat Removal

The Passive Decay Heat Removal (PDHR) [JN02] and the Emergency Core Cooling Systems (ECCS) [JN01] are passive, diverse and segregated and provide multiple means of removing decay heat in response to faults.

All design basis Loss of Coolant Accidents (LOCAs) are protectable by the ECCS [JN01], with diverse protection available from the High-Pressure Injection System (HPIS) [JND] for smaller leaks.

The principal means of delivering the Control of Fuel Temperature (CoFT) LOCA protection function is a passive system that operates without the need for pumps, diesel generators or operator action, as has been employed by active systems on Gen II and Gen III designs. This approach provides a highly reliable system that delivers continues improvement of safety standards and incorporates industry lessons learned, informed by a review of RGP and OPEX. For more information on the ALARP and BAT position regarding heatsinks, see Reference [16].

The decision reviewing heatsink diversity to provide the CoFT safety function, demonstrates that the use of the Local Ultimate Heat Sink (LUHS), as the principal heatsink for the PDHR [JN02] and ECCS [JN01] measures, is consistent with United Kingdom (UK) and international RGP.

It is noted the Automatic Isolation Valves (AIV) (Control and Instrumentation (C&I) actuated) are required to initiate for ECCS [JN01] operation. All the redundancies of the safety class 1 C&I that support the ECCS [JN01] will be protected to ensure that no design basis internal hazard, such as fire or steam leak, can defeat one of the safety class 1 C&I redundancies.

Furthermore, the processing equipment of each redundancy of the class 1 C&I systems will be located in a separate fire zone, supported by its own independent class 1 support services. The safety class 1 C&I cables are separated between redundancies and shall be protected against design basis internal hazards. Periodic testing of safety class 1 C&I shall also be performed in such a way as to maintain adherence to the single failure criterion.

To further reduce risks to ALARP, the ECCS [JN01] can also be initiated by a diverse class 2 C&I system, which can actuate the same actuators, but use a diverse set of sensing parameters to reduce the risk of Common Cause Failures (CCF).

Boron-free Chemistry

Boron-free chemistry minimises the use of substances on the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) list (boric acid and tetraborate salts are identified as a Substance of Very High Concern) and minimises decommissioning activities for systems containing boric acid and tetraborate salts.

With Boron-free, the Shut Down Margin (SDM) and hold-down is achieved by the control rods alone; thus, minimising system complexity and offers a reduction in faults; such as, human error (working on a simplified system). There is an elimination of boron dilution faults: Crud Induced Power Shifts (CIPS); boric acid corrosion and associated radiation fields. With boron-free chemistry there is a simplification of the waste treatment system and an elimination of a boron recycle system (including the evaporator which can lead to high dose exposure and other problems during dismantling), minimising decommissioning waste. Without boron, there is the potential for harmonisation of chemistry across the systems/pools and tanks which interface with the Reactor Coolant System and tritium generation is minimised.

Further evidence is required to demonstrate that the performance of the following systems meet the safety requirements placed on fuel design:

1. The smaller Control Rod Drive Mechanism (CRDM)
2. The increase in cooling demand
3. The increase in columns in upper internals
4. New in-core instrumentation signal transmission method
5. The increase in scope for the Steam Generator design
6. The compatibility of new materials

Sensitivity studies are required for poison loading (intra-assembly poison pin optimisation), uranium enrichment, pin and guide tube location, and through-cycle moderator temperature swings, as this is paramount to the performance of a boron-free equilibrium cycle design. There is a Verification Strategy available to verify reactor performance requirements.

Boron-free fuel handling faults (such as, dropped load of the borated cage during the cask loading process; fuel rod attached to the Integrated Head Package (IHP) during a refuelling lift and the dry long-term storage cask with the use of transport rods to provide reactivity suppression) require safety assessments.

Further work is required to understand the impact on source term from the use of potassium and the availability of directly applicable OPEX; and further studies on the methodologies of fuel crud removal. For more information on the boron-free decision, see Reference [17]. A Boron-free chemistry regime has been selected, further justification and systems design to achieve this regime will be reported in future revision of the E3S Case.

24.3.2 Design Development of Systems

The following section includes some key decisions from the PCD phase of the project at a system level. All design decisions have been developed in accordance with the systems engineering design process (see Section 24.2 and E3S Case Chapter 3: E3S Objectives and Design Rules for Structures, Systems and Components (SSCs), Reference [18]) which includes alignment to RGP & OPEX, design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant safety criteria to reduce risks to ALARP, BAT and Secure-by-Design.

Mechanical Systems: Reactor Coolant System

Preliminary performance analysis on the RCS [JE] has informed the design development of the RCP [JEB] supporting the inclusion of a flywheel to provide adequate coast down flowrate during early stages of certain design basis faults, including Station Blackout, with early indication that acceptance criteria can be met (further analysis is required for verification).

A pump induced (RCP) spray system design, with connections from two of the cold legs converging into a spray nozzle, has been selected for the pressuriser. Optioneering against other mechanisms (such as surge induced spray) concluded that the pump induced spray represents RGP in comparison with other PWR designs, providing a passive response (with no reliance on moving parts; such as, non-return valves) and a performance with increased margins to core saturation acceptance criteria, for more information, see E3S Case Chapter 5: Reactor Coolant System and Associated Systems, Reference [19].

Mechanical Systems: Passive Decay Heat Removal System

Optioneering of redundancy arrangements of the PDHR [JN02] has resulted in the election of one out of three (1oo3) redundancy for the PDHR cooling train and heat exchanger architecture, to improve the reliability of the system from the earlier 2oo3 design; this design enhancement gives a design that is single failure tolerant following the upstream steam leak and Steam Generator Tube Rupture (SGTR) faults that render one train of the safety measure unavailable to deliver the PDHR function.

Further work requires safety requirements to be placed on either the Power Operated Steam Generator (SG) Relief Valves or Passive SG Relief Valves for secondary pressure control, dependent on further assessment of fault conditions, with consideration of appropriate diversity with the ECCS [JN01]. Hazard protection requirements to ensure the PDHR [JN02] is tolerant to internal and external hazards will also be developed based on further hazards analysis, for more information, see Reference [20].

Additional work to support the on-going design development will be presented in a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

Mechanical Systems: Emergency Core Cooling System

Optioneering of redundancy arrangements of the ECCS [JN01] has resulted in the selection of 1oo3 redundancy for the accumulator architecture and 1oo3 redundancy for the phase 2 gravity drain lines; this decision is based on RGP for improved single failure tolerance over 2oo3 designs, and minimising reliance on structural integrity arguments for RCS pipework. The decision to include accumulators in the ECCS system is consistent with relevant established practice, as a passive means of supporting nuclear safety, with fewer components and a higher reliability solution.

It is noted that there is a potential increase in magnitude from internal hazards (i.e., missiles from larger pressurised vessels) that require addition mitigation measures, such as, barrier and installation features. This work is part of the ongoing Internal Hazards assessment and design work.

There is an additional dose burden associated with the testing and inspection of an ECCS accumulator arrangement but, on balance, it is considered that the benefits of accumulators (PDHR [JN02]) significantly outweigh the detriments compared to a pumped solution, as the time required to initiate pumps would lead to unacceptable period of core uncovery during a LOCA. It is noted other reactor designs for both active and passive emergency core cooling systems include gas pressurised accumulators to allow a rapid reflood of the Reactor Pressure Vessel (RPV) during a LOCA. For more information, see Reference [21].

The on-going design development of the ECCS [JN01] will be presented in a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

Mechanical Systems: Local Ultimate Heat Sink

Various containment cooling options have been considered, including cooling by heat exchangers with dedicated water supply, containment surface spray, or a LUHS located within containment, see Reference [22].

A Passive Containment Cooling (PCC) heat exchanger located within containment and cooled by the LUHS has been selected as the preferred option, based on reduced complexity and RGP, with other options being considered, such as, an integrated LUHS (unproven for PWR designs) and containment sprays adding significant complexity with respect to structural support and spray distribution.

The LUHS [JNK] cooling capability is shared between both the ECCS [JN01] and PDHR [JN02] protective safety measures (for the decision file on the shared use of LUHS tanks, see Reference [23]) as well as the mitigative safety measure In-Vessel Retention (IVR) [JMB] (in development).

Further design work is required to optimise the LUHS tank size (e.g., water volume), configuration, and location, alongside performance assessments to determine the decay heat profile to provide the necessary decay heat removal and the long-term cooling requirements **{REDACTED FOR PUBLICATION}**.

Cross connects are provided between tanks **{REDACTED FOR PUBLICATION}** to enable the unused water in one tank to drain to another tank. If one train is unavailable, each interconnect contains two remote isolation valves to protect each train against faults occurring on adjacent trains.

Each tank includes fill and drain lines for system operation. During normal operations, the tank is filled with demineralised water by the Balance of Plant (BoP) Demineralised Supply System [GCH].

Coolant is drained to the BoP waste liquid drains, a second fill connection allows diverse water supplies to be temporarily aligned to the LUHS to provide continued decay heat removal beyond 72 hours, when the initial inventory has boiled off; this connection is assumed to be isolated during normal operations with a threaded cap.

In an emergency, this can be manually opened and aligned to the safety measure coolant supply system which can draw water from a variety of sources, such as, the deaerator, mobile tanks and the Potable Water Distribution System [GHA]. For more information on the LUHS configuration, see Reference [16] and E3S Case Chapter 6: Engineered Safety Features, Reference [20].

Mechanical Systems: Emergency Boron Injection

The decision of selecting the HPIS [JND], to inject boron into the RCS [JE], as part of the Alternative Shut-down Function (ASF) [JD02] was taken to minimise spurious boron dilution faults and reduced complexity in the design to enable Examination, Maintenance, Inspection and Testing (EMIT) activities.

The use of a pump and boron storage tank arrangement was selected over options such as borated accumulators or a powdered boron tank to reduced complexity of the ECCS [JN01] and reduced potential for boron crystallisation (or undissolved boron powder) leading to failure of valves or pumps.

Further design and performance analysis is required to confirm that the HPIS [JND] can meet both the requirements of ASF [JD02] and PDHR [JN02]. As such, the option for ASF [JD02] to utilise a dedicated high-head pump for boron injection remains open. It is worth noting that the HPIS [JND] is not ASF [JD02] specific and is required to support PDHR [JD02] operation during small LOCAs. For more information, see E3S Case Chapter 6: Engineered Safety Features, Reference [20].

Electrical Systems: Electrical Power System

Optioneering the design of the Electrical Power System [B] and Standby Alternating Current (AC) Power Supply architecture has resulted in two redundant divisions each powered by a single power source for the baseline design, on the basis that it aligns to RGP & OPEX for Class 2 systems on other PWR designs (such as AP1000), and it aligns to the Class 2 two-train safety systems that it will supply power to during a Loss of Off-site Power (LOOP) (e.g., HPIS [JND]).

The electrical system has two redundancies for the main generator-backed supplies (Divisions 1 & 2), however, there are more than two redundant divisions at the lower levels.

Low Voltage Essential AC Division 1 connects to battery-backed supplies 1 & 2 and Low Voltage Essential AC Division 2 connects to battery-backed supply 3 with an alternative supply route interlinked to avoid cross connection to battery-backed supply 2.

Additional options for power source arrangements, such as dual redundant power sources for each division or an additional Class 3 ‘spare’ power source, remain open with further optioneering and down-selection expected as the design develops. Technology options for the

Standby AC Power Supply power sources also remain open at PCD, with options including diesel generators, gas turbine generators and generators using low emissions fuel being explored. For more information, see E3S Case Chapter 8: Electrical Power, Reference [24].

Electrical Systems: Uninterrupted Power Supply

The architecture of the Uninterrupted Power Supply (UPS) to supply the Reactor Island C&I systems has been developed to ensure appropriate redundancy and resilience to faults. The selected design option ensures that every essential RR SMR system will be given its own battery backed supply if required, with no sharing of batteries across different classified C&I systems or other essential systems, and for safety class 1 & 2 systems, each redundancy has its own separate battery backed supply. This follows RGP and OPEX from the E3S Principles (see Reference [2]), electrical codes and standards and aligns to electrical systems in other PWR designs.

The Reactor Safety C&I and the essential switchboards will also incorporate 50% dual parallel redundant batteries, to provide further resilience and ensure that failure in one division will still allow loads to be supplied. For more information, see E3S Case Chapter 8: Electrical Power, Reference [24].

Control & Instrumentation: Reactor Plant Control and Monitoring

Options for single, two, three, and four levels of redundancy have been explored for the Reactor Plant Control and Monitoring System (RPCMS) [JS] cabinets and communication networks to perform duty and preventive safety functions, with the selection of dual redundancy. This is on the basis that two redundancies provide the optimised position with respect to achieving probability of failures on demand (pfd) targets and minimising the demand on the protection C&I systems Reactor Protection System (RPS) [JRA] and Diverse Protection System (DPS) [JQA], whilst meeting RGP that no single failure will take the plant offline.

Compared to higher levels of redundancy, the design offers the benefit of minimising the complexity of operation and EMIT, as well as the overall power demand for the system. Clearly higher levels of redundancy offer increased tolerance to faults; however, the safety benefit is expected to be limited due to CCFs and the increased level of complexity, increasing the likelihood of spurious failures; this approach aligns to RGP which focuses on increased reliability for Class 1 and 2 systems.

For sensors, triple redundancy on each measurement has been selected for the current design baseline to ensure that for conflicting valid sensor readings the control system is able to determine which reading is suspect, which is simpler to achieve with three sensors than two. As the redundancy is for reliability purposes rather than single failure tolerance, no separation of signals is needed, all 3 measurements will be made available to each control system redundancy, noting that separate and diverse signals are provided for delivery of the highly categorised safety functions. Further work will be undertaken as the design progresses to confirm this position. For more information, see E3S Case Chapter 7: Instrumentation and Control, Reference [25].

Control & Instrumentation: Diverse Protection System

Key DPS [JQA] design decisions include a hardwired technology to achieve system requirements, on the basis that a hardwired system follows UK RGP in providing a diverse technology to software-based technologies used in the RPS [JRA]. It also provides a simplified

solution with respect to potential failure modes and the verification and validation of the system. A hardwired system is also less vulnerable to cyber security risks than a software-based system. For more information, see E3S Case Chapter 7: Instrumentation and Control, Reference [25].

At PCD, the DPS [JQA] redundancies and voting logic is 2oo3. The benefits of a 2oo4 system are being explored to improve reliability and single failure tolerance. The outcomes of associated design decisions will be reported in a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

Control & Instrumentation: Human Machine Interfaces

The design of Human Machine Interfaces (HMI) in the control rooms and procedures used to verify and validate the functional design are based on RGP. Hardwired and computerised HMI have been considered for the RR SMR, with the current design baseline being an HMI solution that is predominantly computerised that has a robust hardwired back-up for a sub-set of important safety displays and controls.

This option has been selected following an extensive review of RGP and OPEX from other PWR designs and is considered to maintain Defence in Depth (DiD) and achieve required reliabilities, as it includes both RPS operator terminals and Class 1 DPS controls and displays in both the Main Control Room (MCR) and Supplementary Control Room (SCR).

The design also represents a simplified solution compared to a full hardwired back-up system, which is consistent with existing practice seen on other PWR designs, noting that different solutions are adopted dependent on national regulations, including both full and minimal hardwired back-up HMI. For more information, see E3S Case Chapter 7: Instrumentation and Control, Reference [25].

Auxiliary Systems: Storage Ponds

The design decision for the Storage of Spent/Irradiated Fuel Assemblies and Other Radioactive Parts System [FAB] selects storing fuel in ponds and dry casks. Criticality prevention is assured through a combination of geometric fuel spacing and fixed neutron absorption, which is consistent with relevant good practice demonstrated on modern boiling water reactor plants. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26]

Auxiliary Systems: Fuel Transfer Channel

The design of the Fuel Transfer Channel [FCK] and the concrete structure around the metal tube is still in development. Outstanding work includes the shielding and containment requirements. Both passive and active cooling systems are being explored to determine the most appropriate method to meet cooling requirements following a stuck fuel assembly. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26].

Auxiliary Systems: Refuelling Pool

A traditional flood-up approach for refuelling with a Refuelling Cavity [FAE] sluice gate for reduced IHP lift height is the selected design option for the Refuelling Pool [FAF] and Refuelling Cavity [FAE] system, as it represents RGP for PWRs in comparison to other more novel options, such as a shielded and cooled transfer container.

The design has safety benefits over other options considered, including a simplified design e.g., no challenging cooling water connections or integrated lifting system for a shielded transfer container, and a large water volume provides longer grace-times for fuel cooling in the event of a cooling system failure.

The Refuelling Pool [FAF] is designed to store partially burnt up fuel only, which will be returned to the RPV, rather than sized to permit storage of the full core load. Whilst adding a small increase to refuelling time, the partially spent fuel does not need to be lifted into the fuel transfer system and transferred to the Spent Fuel Pool (SFP) [FAB10], and fully spent fuel does not need to be temporarily stored on route to the SFP [FAB10], thus reducing the overall number of fuel assembly lifts and upender transits and minimising the risk of a dropped fuel assembly. The design also reduces the overall volume of the pool, reducing the volume of tritium generated in the pool. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26].

Auxiliary Systems: Main Cooling Water System

Main Cooling Water System (MCWS) [PA] architecture has been developed with two independent trains, combined with the selection of highly reliable pump technology and each train having multiple mechanical draught cooling tower cells; this decision has been made to support a higher system reliability to reduce the potential for loss of the duty cooling function during operation. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26].

Auxiliary Systems: Component Cooling System

Early optioneering for the Component Cooling System (CCS) [KAA] architecture has considered the varying levels of redundancy in the system, including options for a single train, two segregated trains, two trains with a common header, or two trains cross-connected. A cross-connected system was selected on the basis that it reduces the potential for single points of failure and increases reliability of the system. Furthermore, it allows a controlled shutdown and continued cooling following failures. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26].

Auxiliary Systems: Essential Service Water System

Essential Service Water System (ESWS) [PB] baseline architecture has been developed with a two-loop cooling system utilising a Wet Closed Mechanical Induced Draught Cooling Tower, on the basis that it reduces system complexity and potentially improves system reliability, whilst it also reduces cost, minimises footprint, provides better thermal performance, and increases the potential for standardisation and modularisation. The selected baseline maintains three barriers to the release of contamination to the environment, and it reduces construction materials and energy during operations with no expected increase in radioactive discharge to the environment.

Optioneering of the water source to provide make up for evaporative losses has resulted in provision by the BoP Water Supply System [GA]. This is potable water which can be provided by normal domestic water supply or supplied passively from a water tower (by gravity) with capacity sufficient for 72 hours operation; there is a water tower system per train of the ESWS and they are separated and segregated from one another. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26].

Auxiliary Systems: Auxiliary Cooling and Make-up System

The Auxiliary Cooling and Make-up System (ACMS) [PE] architecture has been developed with one train with the filtration structure and ACMS pumphouse utilises two independent flow channels within them, with each significant piece of equipment (trash rack, submerged filter, pump) having a standby unit. Each standby unit can deliver 100% of the make-up flow, which can be brought online with minimal loss of supply to the interfacing systems. This redundancy arrangement will increase the availability of the system, which in turn will increase the reliability of the plant and reduce the amount of plant trips, therefore have a lower reliance on safety systems. For more information, see E3S Chapter 9A: Auxiliary Systems, Reference [26].

24.3.3 Analysis Informed Design

Deterministic Analysis

E3S uses deterministic analysis techniques to formally identify and assess faults and hazards, to provide requirements for safety measures, and demonstrate their suitability, to reduce radiological doses and risks to levels that are ALARP and to continually inform and improve the RR SMR design.

The systematic process of hazard identification is used to review the developing design, primarily for faults and hazards with nuclear consequences. The timing and level of this review depends on the maturity of the design, see Reference [27].

It is a requirement of the Definition Review (DR) Process C3.2.1-2 that suitable and sufficient E3S assessment is performed before the system enters DR3, where options are down selected to form a single solution.

Hazard Identification studies have been undertaken to inform and develop the design up to PCD (and will continue to be undertaken as the design develops), which has resulted in the identification of risk reduction measures incorporated into the design. Some examples are listed below (non-exhaustive):

1. For the Chemistry and Volume Control System (CVCS) [KB], see Reference [28], consideration of installation of an orifice plate/flow restrictor was identified as a Hazard and Operability study (HAZOP) action to reduce the potential for excessive hydrogen feed

2. Following the activation of the SG relief valve, the HAZOP process identified a potential failure to re-seat, this resulted in the requirement for remote isolation, see Reference [29]

3. To prevent a potential explosion hazard, identified during the HAZOP process, non-oil filled transformers or alternative oils to limit potential environmental consequences were identified as mitigating measures, see Reference [30]

4. The HAZOP process identified a design requirement to provide an indication of abnormal discharges, resulting in an improved tank design that includes conductivity or pH monitoring in the collection and drainage of liquids for systems in controlled/exclusion areas (i.e., Reactor Island) [KTA], see Reference [31]

5. To minimise the risk of cracks within the transfer tube leading to loss of coolant volume, the HAZOP process identified a design improvement that places the refuelling pool-side channel flush with containment wall, see Reference [32]

6. Identification of overflow as potential hazard for the Radioactive Liquid Effluent Processing System [KNF], resulting in consideration of overflow protection on the tanks, see Reference [33]

For the full list of hazard identification studies, see the Hazard Log Report and associated Hazard Log, Reference [34].

The RR SMR Fault Schedule collates Postulated Initiating Events (PIEs) that have been identified and sentenced through the safety analysis process and assigns safety functions which are categorised, then placed onto the SSCs that deliver them through SFRs; the SSCs are then classified based on the highest category function they fulfil.

Within the Fault Schedule, all levels of DiD are considered, including, Level 5: mitigation of radiological consequences of significant releases of radioactive material. Level 5 includes emergency control measures and on and off-site emergency response accident management (such as Radiation (Emergency Preparedness and Public Information) Regulations (REPPIR) and post-accident accessibility.

Deterministic performance analysis (e.g., thermal hydraulic performance, stress analysis etc.) is used to verify the SFRs placed onto SSCs by the Fault Schedule and provide high confidence in their ability to achieve their safety functions. Deterministic analysis evaluates the success of the design against deterministic E3S requirements (deterministic design rules); such as, selection of appropriate codes and standards and single failure tolerance. The deterministic assessment links with environment assessments to determine if risks are reduced to ALARP, using the numerical targets presented in E3S Case Chapter 3: Objectives and Design Rules, Reference [18], for SSCs.

The Fault Schedule is embedded and updated directly within the RR SMR requirements management system, Dynamic Object-Oriented Requirements System (DOORS); this provides a single source of information, reducing error and increases visibility of identified faults and links them directly to the design to support the *golden thread* visibility. This and other digital tools are being developed to facilitate the traceability of deterministic analysis from the design through to operations, including processes to transfer Operational Limits and Conditions (OLCs) into operational documentation.

Probabilistic Analysis

At PCD, the PSA is of limited maturity and scope, reflecting design baselines prior to PCD for Intact Circuit Faults (ICFs) and LOCA plant faults during power operations only.

The calculated Core Damage Frequency (CDF) is significantly below the individual risk and societal risk Basic Safety Objective (BSOs), and therefore provides confidence that the RR SMR design will achieve the numerical safety targets, presented in E3S Case Chapter 3: Objectives and Design Rules for SSCs and Reference [18].

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

PSA has informed the design up to PCD, with sensitivity studies conducted on various design changes which have supported the changes made and demonstrate that they are contributing to reducing risks to ALARP, Reference [35], these include:

1. Passive depressurisation valves have been incorporated into the baseline ECCS [JN01] emergency blowdown lines. These reduce the spurious ECCS [JN01] initiation fault frequency and therefore reducing the predicted CDF.

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

3. Passive water traps for LUHS breathing. Initial PSA demonstrated common mode failure of LUHS breather valves failure to open on demand (previously required to open during LUHS tank water level lowering, in support of injection to the RCS [JE]) as important. Therefore, the functionality provided by the breather valves has been replaced by passive water traps with no mechanical moving parts, providing a significant reliability improvement over breather valves. This has improved the reliability of the ECCS [JN01] functionality, thus reducing the predicted CDF.

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

Internal Hazards Analysis

Internal hazards specialists have been involved early in the design process for the RR SMR programme; setting out key principles and methodologies on which to inform the design and undertake internal hazard assessments.

The compact SMR design requires a detailed and specific consideration of internal hazards due to the potential for event combination and escalation given the separation distance between hazard sources.

Internal hazards assessments consider single random failures, as the internal hazards safety case should be tolerant to the potential for a single random failure. In general, this is addressed by ensuring that a Class 1 system claimed against hazards is itself tolerant to a single random failure. In some cases, it may be appropriate to identify an additional line of protection. For more information see Reference [36].

Internal hazard assessments will generate hazard protection options and implement solutions that demonstrate the risk is reduced to ALARP, this work is on-going but key Internal Hazards (along with solutions and safety measures) will be identified in a future revision of the E3S Case.

At PCD, focus has been on identifying the key hazards within the main areas of Reactor Island [R01], as these areas that contain most of the Class 1 and Class 2 SSCs; these areas include:

1. Containment
2. Interspace
3. Safeguards Fluids Block
4. Safeguards EC&I Block

5. Auxiliary Block
6. Ancillary Block
7. Access Block
8. Fuelling Block

Internal hazards assess each area by using the following set of guide words to generate hazard protection or tolerance options to protect, separate and segregate, as appropriate, to maintain safety functions in the event of hazards, noting assessment work is currently on-going:

1. Fire
2. Explosion
3. Flooding
4. Pipe Whip
5. Steam Release
6. Missile
7. Blast
8. Electromagnetic Interference
9. Dropped Loads
10. Hazardous Materials
11. Vehicular Transport Accidents

High integrity components need to be protected and different divisions or trains of safety systems need to be segregated; this will be achieved using hard boundaries, spatial separation, or a combination of the two, including segregated routing of pipework and cabling.

Layout reviews to identify internal hazards and hazard protection options for each area are on-going, to ensure that the early design incorporates measures to reduce risks of internal hazards to ALARP, which will be confirmed through future analysis work. A summary of the outputs of this work will be presented in a future revision of the E3S Case as evidence in the CAE Route Map, Reference [4], becomes available.

External Hazards Analysis

External hazard studies identify hazards and parameters based on RGP which supports reduction of risks to ALARP; these parameters are incorporated into the RR SMR design.

The hazards from both natural and manmade external events applicable to RR SMR have been determined using techniques provided in RGP and are supported by both national and international guidance. The hazard frequencies for determining the magnitudes of the events have been developed from the ONR SAPs and the level of conservatism has been taken from ONR Technical Assessment Guide (TAG) 13. The values determined in the Generic Site Envelope (GSE), presented in Reference [37], are for plants sited in GB and have been compared against and bound values from previous Generic Design Assessment (GDA) studies, supporting the claim that external hazards follow RGP.

The external hazard parameters will be further examined to ensure that risks are reduced ALARP by carrying out studies reviewing the cliff edge and beyond design basis events as the design programme develops. To determine that the design is balanced, external hazards will also be considered in the PSA.

Several key design features of the RR SMR are being developed to provide protection against external hazards, including the:

1. Hazard Shield, a significant concrete structure providing aircraft impact protection to SSCs which are required to deliver and maintain the plant in a stable, safe state. This is currently anticipated to include the Containment, Fuelling Block (including SFP), and the Safeguards Block (Main Control Room and associated safety critical systems – fluids and C&I). The Hazard Shield is not anticipated to fulfil a secondary confinement function.

2. Base isolation system (within the hazard shield), comprising a concrete pedestal/plinth, supporting a horizontally flexible and vertically stiff Aseismic Bearing (ASB). The ASB decouples the structures above it from ground motion during a design basis earthquake. The SSCs within the hazard shield will be seismically qualified, as required; the base isolation system will reduce the horizontal accelerations experienced by the equipment.

The earth berm (surrounding the site) is also likely to provide flood protection; however, this will be considered on a site-specific basis.

Severe Accident Analysis

For this stage in the design, Severe Accidents Analysis (SAA) will focus on the following three sequences to provide confidence that the design protects against large/early releases; this analysis will be included in a future revision of the E3S Case:

1. Large LOCA - operation of In-Vessel Retention (IVR) with no ECCS

2. Small line break / small LOCA - operation of IVR with no PDHR/ECCS

3. Station Blackout (LOOP) - loss of all non-passive mitigation with no recovery

Analysis on a full suite of severe accident cases for an appropriate level of design maturity will be carried out, as the design matures. The outputs from this work will inform the design by:

1. Determining postulated plant conditions- Determining (approximately) the plant conditions to support the PSA development

2. Providing characterization of Severe Accident (SA) progression - Severe accident justification will provide an idea of the time required to initiate the SSCs recognizing the complexity/difficulty of operation

3. Supporting justification of SSCs - Severe accident justification will support the identification of the equipment necessary to deliver the High-Level Safety Functions (HLSFs). Design Extension Conditions (DEC) B SSCs will be identified based on a review of RGP, optioneering and analysis to determine the best choice for the RR SMR (this process is iterative), SA justification will determine (approximately) the setpoints for parameters which trigger protective systems and allow confirmation that they are effective and allow adequate operating margins

4. Supporting determination of the sizing of SSCs – Modular Accident Analysis Programme (MAAP) analysis will be used to demonstrate that the sizing and number of SSCs is sufficient to deliver the identified safety functions, for example that there will be enough hydrogen igniters/recombiners within containment for worst case severe accident progression

5. Supporting identification of equipment classification - MAAP will be used to provide an idea of the environmental conditions likely during the severe accident, this will be used to justify the classification applied to the identified severe accident SSCs

6. Supporting identification of equipment performance and environmental qualification requirements – by quantifying identified severe accident SSCs to deliver the required functions in conditions expected to be experienced during the severe accident. This provides equipment qualification, in terms of supporting the definition of the operating envelope where equipment is claimed to provide a safety function under severe accident conditions and is qualified to do so

7. Supporting Justification of levels of DiD - During the SA justification, DOORs and Level 2 PSA will be used to demonstrate the independence of the identified severe accident SSCs from other levels of DiD which are likely to have already failed or been bypassed. In addition, SAA will provide justification of the DiD provisions in the design, through identification of any 'cliff edge' effects or demonstration that no 'cliff edge' effects in the accident analysis are seen

8. Supporting Identification of and justification for DiD Level 4 Supporting Systems – Identifying the support systems needed to initiate and maintain the operation of the SSCs (for example, C&I, AC and DC power, heat sinks etc.)

9. Supporting identification of mission times and stock requirements - Analysis will provide an idea of mission times and stock requirements (e.g. water, fuel, DC power) for severe accident SSCs and their associated support systems

10. Supporting emergency arrangements and procedures - SAA will Inform emergency procedures and support the development of accident management strategies, guidelines and procedures considering the adverse working environments that could be seen during and following a severe accident. RR SMR will not provide detailed emergency arrangements or procedures during the GDA process

11. Supporting Level 5 DiD measures

Radiation Protection

Ensuring that radiation exposure of employees and other persons is kept to levels that are below legal limits and are ALARP is a key objective in the design of the RR SMR. The high-level principles adopted by the RR SMR in order to meet the requirements of IRR17 and the design objectives detailed of the RR SMR are presented in the SMR Dose Management Policy, Reference [38], which provides the general dose management principles, relevant legislation and good practice, plant zoning, technical issues and key policy and design interfaces for the RR SMR. It sets out the holistic approach to dose reduction for the RR SMR during critical operation, refuelling outages and EMIT activities whilst the plant is shutdown.

Additional principles specific to radiation shielding and the radioactive source term, including principles specifically intended to reduce dose uptakes to employees and other persons. The

Radioactive Source Term Policy, Reference [39], defines a structured approach to minimising the source term. The Radiation Shielding Policy, Reference [40], provides the general shielding principles, the shielding design process, radiation safety criteria, technical issues, design interfaces and analysis tools/methods

Furthermore, there are a set of guidelines, including contamination zoning, to provide detailed guidance to designers to ensure that the RR SMR plant is designed to reduce doses to employees and other persons SFAIRP, in line with the requirements of IRR17 and regulatory expectations, these guidelines can be found in Reference [41].

Radiological dose rate assessments will provide evidence that the design is compliant with the Policies (set out above) and guidelines have been applied; these assessments will be available to support ALARP demonstration.

Human Factors Analysis

Within this PCD phase, a variety of HF assessments have been completed across the whole scope of RR SMR. Most of the analysis has focused on areas of high complexity, or which are required to reach a greater level of design definition earlier in the design programme. As such, the analysis has focused primarily on Reactor Island [R01] but the analysis outcomes obtained are often applicable or useful across the other islands.

The early involvement of HF on the RR SMR programme has provided a foundation for future assessments, through requirements derivation, identification of key standards and design guidance. Key information which needs to be communicated to the design teams will be captured within the DOORS requirements tool and flowed to each responsible area.

The HF team have produced a HF checklist to provide designers with a structured high-level overview of what a HF competent person would expect to see in the design; this equips the designer with information required to integrate HF into their design from the start of the design process and provides evidence that risks to HF will be reduced to ALARP.

A HF Integration Plan and the following summary documents will be available to support ALARP demonstration: Allocation of Functions, Human Based Safety Claims and Human Reliability Assessments.

Conventional Safety Analysis

To reduce the risk to conventional and fire safety, the Design for Conventional Health and Safety Process C3.2.2-4 and associated Health and Safety Checklist provides guidance on designing for conventional health and safety to engineers.

The Health and Safety Checklist guides users to identify relevant regulations, applicable codes and standards (Approved Codes of Practice (ACoPs), Standards etc.), conventional health and safety hazards and identify mitigation measures within the design to reduce risks to ALARP.

In accordance with Construction Design and Management (CDM) regulations 2015, the client and principal designer ensure arrangements are in place for managing health and safety in design, and to provide pre-construction information relating to health and safety to a Contractor.

The health and safety risk registers provide evidence that mitigation measures are captured within the design to reduce conventional and fire safety risks to ALARP.

Risks to conventional health and safety are considered by multiple stakeholders; the E3S team uses hazard identification techniques to discuss conventional health and safety in HAZOP workshops and the HF techniques include consideration of conventional health and safety; this work is on-going and continually informs design.

24.3.4 Risk Reduction Through-Life

Construction

Rolls-Royce SMR's CDM arrangements ensure risks to health and safety are captured on a conventional health and safety risk register. These risks and mitigating measures will form a health and safety technical file that will be passed over to the construction team prior to starting activities.

Commissioning

The strategies and requirements for commissioning are being developed and embedded into RR SMR early in the design, based on RGP and OPEX, to facilitate the safe commissioning of the RR SMR and support risk reduction to ALARP. Further details are outlined in E3S Case Chapter 14: Plant Construction and Commissioning, Reference [42].

Operations

Operating philosophies are being developed alongside design, and processes being developed to ensure OLCs from the design and safety analysis will be transferred into operational documentation, such that the RR SMR will be operated in line with the design intent and the requirements of the E3S case. Further information is provided in E3S Case Chapter 13: Conduct of Operations, Ref [43], and E3S Case Chapter 16: Operational Limits and Conditions for Safe Operation, Ref [44].

Decommissioning

The preferred decommissioning strategy selected for RR SMR is immediate decommissioning, which is consistent with UK Government policy and guidance, evidenced by The Base Case in Reference [45].

Immediate decommissioning may be able to take advantage of the availability of the knowledge and experience of staff that have operated the facility at the end of operations which may still be available and avoids maintenance/asset care costs over an extended period. Furthermore, adopting this strategy avoids transferring the burden of decommissioning to future generations.

Decommissioning is one of the design criteria when evaluating options in line with the Conduct Design Optioneering Process outlined in Section 24.2, driving the design to consider decommissioning activities as part of the design decision process. Decommissioning principles are developed for RR SMR based on a review of applicable international and national regulations and guidance. The following RR SMR design decisions support decommissioning (and BAT) principles to minimise waste:

1. Boron (and lithium)-free (potassium-based) chemistry: Boron-free chemistry (which is enabled by the use of potassium-based pH control) provides a considerable reduction in tritium generation and greatly increases effluent recycling possibilities/minimisation of liquid discharges in normal operation and removes the requirement for evaporators to process liquid waste (minimising waste), which can lead to high dose exposure and other problems during dismantling.

2. Replacement of heavy-duty evaporator with Reverse Osmosis (RO) followed by vacuum evaporator for volume reduction: This allows 95-98% recycling of effluent, reduces Ion Exchange resin waste, reduces volume of concentrates (as the boron-free chemistry permits a higher volume reduction factor).

3. Decay storage of resins/concentrates: The decay storage of these waste streams (in place of direct disposal) will allow the total Intermediate Level Waste (ILW) volumes from these streams to be reduced significantly.

4. Back-washable filters: This reduces waste packages by 75% (averaged over a 10-year period) by reducing ILW filter packages and reducing overall ILW storage volume. Co-packaging of wet Low Level Waste (LLW) waste: This reduces the total number of LLW packages that will be required for offsite management.

5. Cementation of ILW waste: This provides a flexible, turnkey method for treatment to simplify waste disposal.

It is recognised that the overall RR SMR design provides opportunities for decommissioning, including:

1. The RR SMR design philosophy of modularisation provides significant opportunities for decommissioning, as dismantling, size reduction (where possible) handling, packaging and transportation activities are simplified.

2. The deployment of multiple RR SMR Nuclear Power Plants (NPPs) in the UK (and/or internationally) could provide the opportunity for OPEX, equipment (i.e., dismantling) and technique sharing for different lifecycle phases (including decommissioning), standardisation of decommissioning plans and strategies and radioactive waste processing facilities across multiple sites.

24.4Conclusions

24.4.1 Conclusions

Preliminary evidence is presented to support the overall chapter claim that '*The design of the RR SMR reduces nuclear and conventional safety risks to As Low As Reasonably Practicable through the lifecycle*', which contributes to the overall E3S objective to protect people and the environment from harm, and the demonstration that risks are reduced ALARP.

This report summarises the evidence from across the case, available at PCD, to demonstrate that ALARP is being embedded into the processes early in design stage, leading to outputs of the design that support risk reduction to ALARP. The evidence at PCD supports the position that RR SMR risks can be reduced to ALARP, noting further evidence will be developed as the design progresses in line with the CAE Route Map.

24.4.2 Assumptions & Commitments on Future Dutyholder/Licensee

None identified at this revision.

24.5 References

[1] RR SMR Report, SMR0004294/001, “E3S Case Chapter 1: Introduction,” March 2023.
[2] RR SMR Report, SMR0001603, “Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principle,” 2022.
[3] Industry Radiological Protection Co-Ordination Group, “The Application of ALARP to Radiological Risk: A Nuclear Industry Good Practice Guide,” 2012.
[4] RR SMR Report, SMR0002155/001, “E3S Case CAE Route Map,” March 2023.
[5] Health and Safety Executive, “Health and Safety at Work Act,” 1974.
[6] Office for Nuclear Regulation, “Safety Assessment Principles for Nuclear Facilities,” 2014 edition (Revision 1, Jan 2020).
[7] Health and Safety Executive, “Risk management: Expert guidance - Reducing risks, protecting people - R2P2,” [Online]. Available: https://www.hse.gov.uk/managing/theory/r2p2.htm. [Accessed 14 Jan 2023].
[8] IAEA, “Fundamental Safety Principles,” 2006.
[9] WENRA, “Safety Reference Levels for existing Reactors,” 2014.
[10] Health and Safety Executive, “Ionising Radiation Regulations,” 2017.
[11] RR SMR TS-DD-02, “Decision Record Template”.
[12] RR SMR Report, SMR0003036, “Rolls-Royce SMR Key Objectives and Assessment Criteria,” 2022.
[13] RR SMR IBM DOORS Database, “SMR Decision Register, Module Path: /00_Small Modular Reactor/98 - Integration/02 - Decisions, Module,” [Online]. Available: URL: doors://muklopr-app001:36677/?version=2&prodID=0&urn=urn:telelogic::1-6213bd4e18ff23ee-M-000044e0. [Accessed 16 11 2022].
[14] RR SMR Report, SMR0004334/001, “E3S Case, Chapter:17 Management for E3S and Quality Assurance,” Mar 2023.
[15] RR SMR Report, EDNS01000582661/001, “Design Decision Report – Reactor Plant Layout,” October 2017.
[16] RR SMR Report, EDNS01000953979/001, “UK SMR ALARP and BAT Position Paper Reactor Heatsinks,” March 2021.
[17] RR SMR Report, EDNS01000682203/001, “SMR PCD Phase1a – Decision 16 – Boron Free Studies,” July 2018.
[18] RR SMR Report, SMR0004589/001, “E3S Case Chapter 3: E3S Objectives & Design Rules,” March 2023.
[19] RR SMR Report, SMR0003984/001, “E3S Case Chapter 5: Reactor Coolant System & Associated Systems,” March 2023.
[20] RR SMR Report, SMR0003771/001, “E3S Case Chapter 6: Engineered Safety Features,” March 2023.
[21] RR SMR Report, EDNS01000548215, “LOCA Accumulator Decision File”.
[22] RR SMR Report, EDNS01000611164/001, “SMR PCD Phase 1 - Decision 4 - DHR and LOCA Configuration and Sizing,” February 2018.
[23] RR SMR Report, SMR0000626/001, “R01-054 Passive Decay heat removal Architecture Design File.”.
[24] RR SMR Report, SMR0004010/001, “E3S Case Chapter 8: Electrical Power,” March 2023.

[25] RR SMR Report, SMR0003929/001, “E3S Case Chapter 7: Instrumentation & Control,” March 2023.
[26] RR SMR Report, SMR0003863/001, “E3S Case Chapter 9A: Auxiliary Systems,” March 2023.
[27] RR SMR Report, SMR0001228, “HAZID Strategy,” 2022.
[28] RR SMR Report, EDNS01000962402, “Chemical Volume and Control System HAZID,” 2021.
[29] RR SMR Report, EDNS01000692860, “Steam Gerneration Support System HAZID,” 2021.
[30] RR SMR Report, EDNS01000963497, “Turbine Island Missile Protection HAZID,” 2021.
[31] RR SMR Report, SMR0000869, “Initial Concept Hazard Identification Study for the Reactor Island Collection and Drainage System,” 2022.
[32] RR SMR Report, SMR0003390, “Fuel Transfer System Structured What-If Technique,” 2022.
[33] RR SMR Report, SMR0003464, “Final Concept Definition (FCD) Hazard and Operability (HAZOP) 2 Study for the Effluent Processing and Drains System,” 2022.
[34] RR SMR Report, SMR0001317, “Rolls-Royce SMR Hazard Log Report,” 2022.
[35] RR SMR Report, EDNS01000537027, “SMR Probabilistic Safety Assessment”.
[36] Atkins, SMR-SNC-A21-XX-RA-4U-0001, Issue 1, “Redundancy and the Single Failure Criterion,” July 2020.
[37] RR SMR Report, SMR0004542/001, “E3S Case Chapter 2: Generic Site Characteristics,” March 2023.
[38] RR SMR report, SMR0000635/001, “Small Modular Reactor Dose Management Policy,” 2022.
[39] RR SMR Report, SMR0000512/001, “Small Modular Reactor Radioactive Source Term Policy,” July 2022.
[40] RR SMR Report, SMR0000636/001, “Small Modular Reactor Radiation Shielding Policy,” May 2022.
[41] RR SMR Report, SMR0001861/001, “Radiation Protection Design Guidelines for the RR SMR”.
[42] RR SMR Report. SMR0004289/001, “E3S Case Chapter 14: Plant Construction and Commissioning,” March 2023.
[43] RR SMR Report, SMR0004247/001, “E3S Case, Chapter 13: Conduct of Operations,” March 2023.
[44] RR SMR Report, SMR0004555/001, “E3S Case, Chapter 16: Operational Limits and Conditions for Safe Operation,” March 2023.
[45] EUR, “European Utility Requirements LWR Nuclear Power Plants Volume 2 Generic Nuclear Island Requirements, Chapter 4: Design Basis, Revision E,” October 2016.

24.6Appendix A: CAE Route Map

24.6.1 Chapter 24 Route Map

A preliminary Claims decomposition from the overall Chapter 24 Claim is summarised in Table 24.6-1, including the Tier 2 Evidence underpinning the Claims at PCD (i.e., summarised in Revision 1 of this report) and further Tier 2 Evidence still to be developed.

Table 24.6-1: CAE Route Map

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 24**	**Underpinning Tier 2 Evidence** ***at PCD**	**Underpinning Tier 2 Evidence** ***to be developed**
ALARP methodology informing design of the RR SMR has been developed based on RGP	-	-	Methodology covers ALARP and optimisation with BAT and Secure-by-Design	Section 24.2	C3.2.2-2 Conduct Design Optioneering Process and Decision Making Template TS-DD-02 [11] E3S Design Principles [2]	As PCD
RR SMR design is developed to reduces risks	SSCs are designed to reduce risks to ALARP	-	Design has followed ALARP methodology, captured in design decision files	Section 24.3.1 and 24.3.2	E3S Case Chapters: 4, 5, 6, 7, 8, 9, 10, 11, 12	ALARP Summary Report

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 24	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
to ALARP through the operational life	Safety analysis has informed the RR SMR design to reduce risks to ALARP	Deterministic safety assessments have informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 15	ALARP Summary Report
		Probabilistic safety assessment has informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 15	ALARP Summary Report
		Internal Hazards assessment has informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 15	ALARP Summary Report

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 24	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
		External Hazards assessment has informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 15	ALARP Summary Report
		Severe accident analysis has informed the RR SMR design to reduce risks ALARP	-	n/a	n/a	
		The RR SMR design permits the delivery of emergency response actions	-	n/a	n/a	ALARP Summary Report
		Radiological exposure assessment has informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 12	ALARP Summary Report

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 24	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
		Conventional Safety assessment has informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 22	ALARP Summary Report
		Human Factors assessment has informed the RR SMR design to reduce risks to ALARP	-	Section 24.3.3	E3S Case Chapter 18	ALARP Summary Report
RR SMR facilitates the reduction of the reduction of nuclear and conventional	RR SMR facilitates the reduction of nuclear and conventional safety risks during construction	-	-	Section 24.3.4	E3S Case Chapters: 14, 22	ALARP Summary Report

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 24	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
safety risks through the lifecycle	RR SMR facilitates the reduction of nuclear and conventional safety risks during commissioning	-	-	Section 24.3.4	E3S Case Chapter 14	ALARP Summary Report
	RR SMR facilitates the reduction of nuclear and conventional safety risks during operation	-	-	Section 24.3.4	E3S Case Chapters: 13, 16	ALARP Summary Report
	RR SMR facilitates the reduction of nuclear and conventional safety risks during decommissioning	-	-	Section 24.3.4	E3S Case Chapter 21	ALARP Summary Report

24.7 Acronyms and Abbreviations

1oo3	One out of three
ACMS	Auxiliary Cooling and Make-up System
ACoP	Approved Codes of Practice
AIV	Automatic Isolation Valves
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
ASF	Alternative Shut-down Function
BAT	Best Available Techniques
BoP	Balance of Plant
BSO	Basic Safety Objective
BWR	Boiling Water Reactor
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CCF	Common Cause Failures
CDF	Core Damage Frequency
CCS	Component Cooling System
CDM	Construction Design and Management
CIPS	Crud Induced Power Shifts
CoFT	Control of Fuel Temperature
CRDM	Control Rod Drive Mechanism
CVCS	Chemistry and Volume Control System
DiD	Defence in Depth
DR	Definition Review
DOORS	Dynamic Object-Oriented Requirements System
DPS	Diverse Protection System
E3S	Environment, Safety, Security and Safeguards
ECCS	Emergency Core Cooling System
EMIT	Examination, Maintenance, Inspection and Testing

ESWS	Essential Service Water System
GB	Great Britain
GDA	Generic Design Assessment
GSE	Generic Site Envelope
HAZOP	Hazard and Operability Study
HF	Human Factors
HMI	Human Machine Interfaces
HPIS	High Pressure Injection System
IAEA	International Atomic Energy Agency
ICF	Intact Circuit Faults
IEF	Initiating Event Frequencies
IHP	Integrated Head Package
ILW	Intermediate Level Waste
IRR	Ionising Radiations Regulations
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
LUHS	Local Ultimate Heat Sink
MAAP	Modular Accident Analysis Programme
MCR	Main Control Room
MCWS	Main Cooling Water System
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NRV	Non-Return Valve
OLC	Operating Limit and Condition
ONR	Office for Nuclear Regulation
OPEX	Operating Experience

PCC	Passive Containment Cooling
PCD	Preliminary Concept Definition
PCSR	Pre-Construction Safety Report
PDHR	Passive Decay Heat Removal
pfd	probability of failure on demand
PIE	Postulated Initiating Events
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
R2P2	Reducing Risks Protecting People
RCS	Reactor Coolant System
RD	Reference Design
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
REPPIR	Radiation (Emergency Preparedness and Public Information) Regulations
RGP	Relevant Good Practice
RPS	Reactor Protection System
RR SMR	Rolls-Royce Small Modular Reactor
RPV	Reactor Pressure Vessel
SAPs	Safety Assessment Principles
SCR	Supplementary Control Room
SDM	Shut Down Margin
SFAIRP	So Far As Is Reasonably Practicable
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SSC	Structure, System and Component
TAG	Technical Assessment Guide
UK	United Kingdom
UPS	Uninterrupted Power Supply
WENRA	Western European Nuclear Regulators Association
WNA	World Nuclear Association