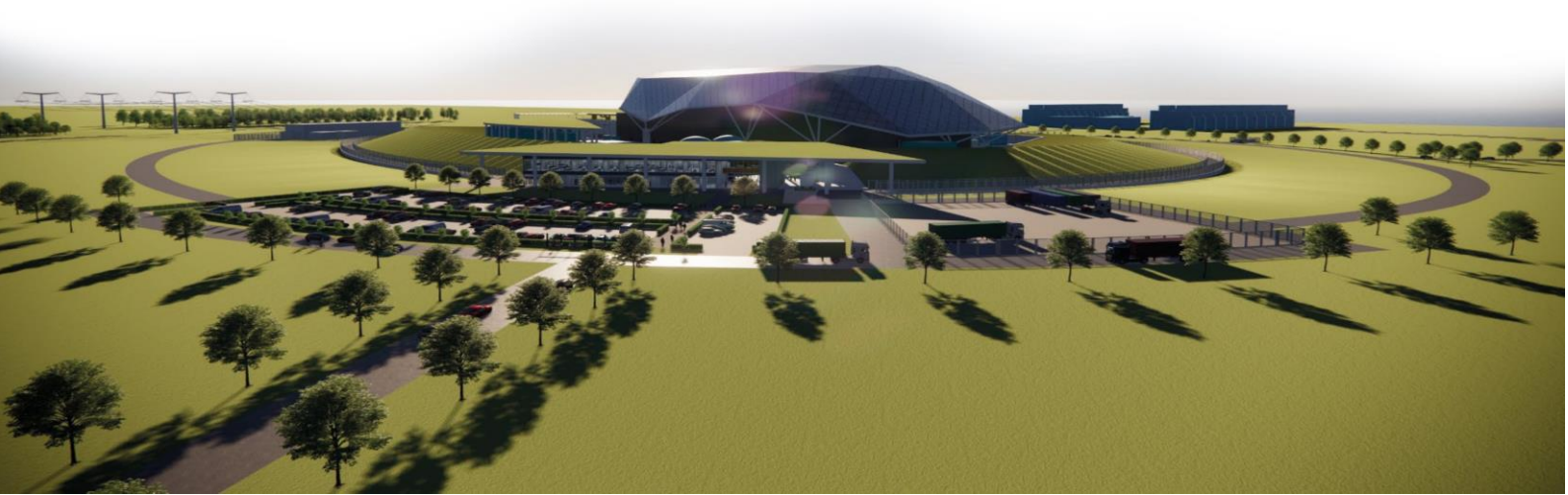
Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 24: ALARP Summary



Record of Change

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First issue of E3S Case
February 2024	2	Issue	It presents a holistic summary of the ALARP position with respect to achieving the generic E3S Case objective, based on arguments and evidence available at Reference Design 7, aligned to Design Reference Point 1.
May 2024	3	Issue	Updated to correct revision history status at Issue 2. Chapter changes include: • Clarification on reference design basis for analysis (section 24.1.2) • Clarification on ALARP methodology and embedding ALARP in E3S and engineering processes (section 24.2.2) • Update to probabilistic safety assessment discussion to align with Chapter 15 • Additional detail within conclusion section for how arguments and evidence presented meet the generic E3S objective Also minor template/editorial updates for overall E3S Case consistency.

Executive Summary

Chapter 24 of the Environment, Safety, Security, and Safeguards (E3S) Case presents the overarching summary of how the Rolls-Royce Small Modular Reactor (RR SMR) can reduce risks to as low as reasonably practicable (ALARP). The chapter outlines the arguments and evidence to underpin the top-level claim that the RR SMR design permits construction, commissioning, operation, maintenance and decommissioning with risks and exposures reduced to ALARP.

The RR SMR ALARP principles broadly cover relevant good practice (RGP), design optioneering, risk assessment, and implementation of improvements. These principles are embedded into the E3S and engineering processes.

At the plant level, the selection of PWR technology for the RR SMR offers a vast amount of RGP and operating experience (OPEX). The layout is being developed with input from E3S to ensure high levels of inherent safety to eliminate risks. Significant defence in depth is provided through safety measures across all five levels, including the provision of two independent and diverse safety measures for protection against frequent faults.

The design of all structures, systems, and components (SSCs) is developed in accordance with the systems engineering design process. This includes alignment to RGP and OPEX, design to codes and standards according to their safety classification, and the extensive systematic optioneering process with down-selection of design options based on assessment against relevant E3S criteria. Safety measures are also designed in line with principles for a simple and forgiving design and the application of the hierarchy of controls, increasing reliability, and reducing the maintenance burden.

Innovative design features are adopted with a view of improving safety and reducing risks, including boron-free chemistry, base isolation, emergency blowdown (EBD) for emergency core cooling (ECC) [JN01] operation, and modularisation to enable build certainty. These design features have the potential for significant safety benefits and risk reduction.

A suite of safety analysis is used to inform the design and evaluate risks against numerical criteria, including deterministic, probabilistic, hazards, severe accident, radiation protection, human factors, and conventional and fire analyses. The analysis concludes that the design is capable of achieving numerical targets and can reduce risks to ALARP.

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 and to achieve the objective of the generic E3S Case.

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 presents the overarching summary of how the RR SMR can reduce risks to as low as reasonably practicable (ALARP).

The RR SMR has an E3S fundamental objective 'to protect people and the environment from harm' [1]. The objective of the generic E3S Case 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 [2]. The ALARP demonstration is key to providing this confidence within the E3S Case.

The purpose of this chapter is therefore to provide a holistic demonstration of how the RR SMR is managing risks to ALARP as it is progressed into detailed design.

24.1.2 Scope and Maturity

The scope of the ALARP chapter covers all aspects of nuclear and conventional safety. The scope covers the full lifecycle of the RR SMR including how the design facilitates risk reduction during future lifecycle stages.

The scope of this chapter covers the RR SMR ALARP process, as well a summary of the outputs from the process to demonstrate how ALARP is embedded within the RR SMR design. This chapter presents a holistic view with a focus on how higher risk or novel design aspects are being managed, with reference to relevant Tier 1 chapters and Tier 2 documents of the E3S Case where more detailed arguments and evidence are presented. The ALARP Summary Report [3] is the primary Tier 2 document underpinning this chapter (the tiered structure of the E3S Case is described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [2]).

Version 2 of the generic E3S Case is based on reference design 7 (RD7), corresponding to design reference point 1 (DRP 1) for the generic design assessment (GDA). Given the iterative nature of the E3S analyses, the analysis outputs are generally based on an earlier design baseline that has informed the RD7/DRP1 design. This is relevant for the following analysis described within this chapter:

- Deterministic modelling of faults is based on RD6 maturity
- Severe accident analysis of design extension condition sequences is based on RD6 maturity
- Probabilistic safety assessment (PSA) inputs are based on an RD6 level of design maturity and the fault schedule developed at RD5 maturity
- Internal hazards analysis for Reactor Island is based on RD6 maturity
- Radiation protection dose and shielding assessments are based on the RD6 layout and design.

24.1.3 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 [2]. The associated top-level chapter claim for E3S Case Version 2, Tier 1, Chapter 24: ALARP Summary is:

Claim 24: The RR SMR design permits construction, commissioning, operation, maintenance and decommissioning with risks and exposures reduced to ALARP

A decomposition of this claim into sub-claims and mapping to the relevant Tier 2 and Tier 3 information containing the detailed arguments and evidence, is presented in the E3S Case Route Map [4]. Given the evolving nature of the E3S Case alongside the maturing design, the underpinning arguments and evidence may still be developed in 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 RD7/DRP1 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 24.8).

24.1.4 Applicable Regulations, Codes and Standards

The following references provide key guidance and relevant good practice (RGP) for ALARP:

- Health and Safety Executive, Health, and Safety at Work Act [5]
- Office for Nuclear Regulation (ONR), Safety Assessment Principles (SAPs), includes numerical targets and safety limits: Basic Safety Objectives (BSO) and Basic Safety Limits (BSLs) [6]
- ONR Technical Assessment Guide: Regulating duties to reduce risks to ALARP [7]
- Health and Safety Executive, Reducing Risks, Protecting People (R2P2) provides guidance on the process of decision making, including risk assessment and risk management [8]
- International Atomic Energy Agency, Fundamental Safety Principles [9], Safety Standards, and Technical Documents
- Western European Nuclear Regulators Association (WENRA), Safety Reference Levels for Existing Reactors [10]
- Health and Safety Executive, Ionising Radiation Regulations [11]
- The Application of ALARP to Radiological Risk [12].

24.2 ALARP in Decision Making Process

24.2.1 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. The terms SFAIRP and ALARP mean essentially the same thing and at their core is the concept of 'reasonably practicable'.

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 term 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, used to define the principle of minimising radiation exposure. In GB, the terminology is broadly synonymous, with both ALARA and ALARP incorporating considerations on economic, environmental, and societal factors. Within the RR SMR E3S Case, the terminology ALARP is used when relating to minimisation of risk, noting ALARA is used within 'environment' chapters of the E3S Case when relating to impacts of waste and discharges.

24.2.2 Methodology

The RR SMR ALARP principles are described in the E3S design principles [1], broadly covering:

1. RGP
2. Optioneering
3. Risk Assessment
4. Conclusion that no further reasonably practicable improvements could be implemented.

These ALARP principles are embedded in the E3S and engineering processes, including the conduct design optioneering process and associated design decision record template used to capture design decision making [13].

The conduct design optioneering process includes the 20 key design objectives and criteria against which the design options are evaluated, described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [2]. Pre-defined weightings associated with each of the criteria provides a consistent measure for design decisions that ensures E3S, and other business strategic objectives, are met.

A comprehensive review of RGP and operating experience (OPEX) forms part of all RR SMR optioneering studies, recorded in the design decision record, that marshals the presentation of this information together to present the arguments and evidence in support of decisions reducing risk to ALARP.

Evaluation of options also includes an assessment of risk against E3S criteria, such as their impact on fault and hazard sequences, numerical safety targets, and dose impacts. E3S stakeholders support this risk evaluation and decision analysis to inform down-selection of design solution(s). All design decisions are documented in the RR SMR Decision Register [14].

As selected options are developed up to and beyond RD7/DRP1, risk is continuously assessed through progressive and iterative safety analysis, as set out in the E3S Requirements and Analysis Arrangements [15] and the supporting suite of standards. This process may lead to revisiting optioneering decisions and design iteration to support the demonstrate ALARP.

Further information on the ALARP methodology is presented in the ALARP Summary Report [3].

24.2.3 Optimisation of ALARP with BAT, Secure by Design and Safeguards by Design

Traditionally, safety, security, safeguards, and the environment have been considered separately within both the design process and regulatory assessment. Each of these topics, however, has the same goal ‘to protect people and the environment from harm’ [1]. For RR SMR, the E3S informed design processes and guidance (for example, the design optioneering process described in section 24.2.2, and the hazard identification process) support a combined ALARP, BAT, secure by design and safeguards by design approach to ensure all E3S aspects are considered and any potential conflicts are managed through the design process. As such, the outputs of the design development process provide a common evidence base for the E3S Case.

24.3 Key Design Aspects

24.3.1 Overall Plant Design

Fundamentally, the RR SMR uses pressurised water reactor (PWR) technology and industry standard uranium fuel. A PWR is selected over other reactor types as it is an established technology that has been demonstrated to be safe, with many operating PWRs globally. The Rolls-Royce SMR Limited organisation also have a vast amount of OPEX in designing, manufacturing, installing, testing, commissioning, maintaining and refurbishing PWRs (see E3S Case Version 2, Tier 1, Chapter 1: Introduction [2]).

In the early stages of the RR SMR development, the fundamental configuration of the reactor coolant system (RCS) was subject to optioneering, with two, three and four loop options evaluated. The three-loop RCS configuration selected is on the basis that it offers an optimised, compact plant layout that minimises the footprint of the Reactor Island compared to RCS configurations with more loops, whilst providing safety benefits through increased redundancy over RCS configurations with fewer loops.

The use of RGP is one of the key ALARP principles (section 24.2.2), and the significant RGP, OPEX and learning available for PWRs that is being used to develop the RR SMR design provides a high-level of confidence that risks can be reduced to ALARP.

24.3.2 Layout

The RR SMR site and plant layout are being developed to underpin E3S claims from across the E3S Case, including internal hazards, external hazards, conventional safety, radiation protection, human factors etc. To underpin the high-level layout claims made in each E3S Case chapter, more detailed E3S requirements or constraints are allocated to the layout. The E3S requirements/constraints are then implemented into the layout as part of the iterative design process.

Examples of E3S requirements/constraints for layout include non-functional requirements such as ‘while in all modes of operation, the pipe run [FAK-PO-05] shall have a cumulative straight length equivalent less than or equal to x m’, which is derived from RGP to support the safety categorised functional requirement for the fuel pool cooling system to remove heat from the fuel pool coolant.

Other examples include non-functional system requirements for each topic area, such as ‘radiation sources shall be segregated from occupied spaces’ for radiation protection, or ‘redundant trains of measures shall feature segregation between them where reasonably practicable’ for internal hazards.

An extensive set of E3S requirements and constraints are developed that have informed the layout at RD7/DRP1, supplemented by strategies and guidance from across E3S topic areas to inform the layout decision making process. These E3S requirements will continue to be refined as the detailed design continues to develop and as further E3S analysis is undertaken.

The E3S requirements are addressed within the layout, taking cognisance of the hierarchy of controls, with the intention of eliminating risks where practicable. Examples of layout design features at RD7/DRP1 that have been informed by E3S requirements to reduce overall risks include:

- Spatial separation of the four trains of the highly safety classified electrical, control and instrumentation (EC&I) around the outside of interspace, segregated through separate civil structural fire compartments, to provide protection against internal hazards (see section 24.4.3 for further discussion on internal hazards).

- Locating buildings containing highly safety classified SSCs within the hazard shield and on the aseismic bearing to protect against design basis external hazards (see section 24.4.4 for further discussion on external hazards).

- Clear delineation of radiation controlled areas (RCA) and non-RCA, with the health physics laboratory in the Access Block on the main personnel route into the RCA, to minimise exposures to workers (see section 24.4.6 for further discussion on radiation protection).

The layout design approach also provides the opportunity to evaluate competing E3S requirements through the conduct design optioneering process (described in section 24.2.2), to make risk-informed decisions that result in an optimised layout that balances risks.

Whilst the layout design is maturing at RD7/DRP1, the design approach ensures E3S requirements are iteratively feeding into the layout solution, which provides confidence that risks can be reduced to ALARP as the design is developed from concept into detailed design. The design approach ensures high levels of inherent safety and risk-informed optimisation is adopted early within the layout design, promoting elimination of risks rather than 'back-fitting' engineered or administrative measures to control risks at a later stage when the layout has been 'finalised'. This follows the hierarchy of controls principle and is a key to demonstrating that the RR SMR layout reduces risks to ALARP.

Further details of the layout design process, E3S requirements and constraints, and a summary of how the layout design at RD7/DRP1 has been informed by E3S, is provided in the Reactor Island Architectural and Layout Summary Report [16].

24.3.3 SSC Design

The design of all SSCs is developed in accordance with the systems engineering design process. This includes alignment to RGP and OPEX, design to codes and standards according to their safety classification, an extensive 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 (see section 24.2.2), and verifying analysis.

Furthermore, the E3S design principles [17] have been used to guide and inform the ongoing design development process. As part of the systems engineering approach, a comprehensive set of non-functional system requirements have been developed from these principles, which are applied by the engineering teams to the site, plant, or SSC as part of the requirements definition during the design process [18]. The requirements cover key design principles such as reliability, single failure tolerance, diversity of initiation between safety measures, and facilitation of Examination, Maintenance, Inspection and Testing (EMIT).

The application of the systems engineering design processes and development against E3S requirements provides underpinning evidence that demonstrates how the design of individual SSCs reduces risks to ALARP. For example, the safety class 1 Emergency Core Cooling (ECC) [JN01] safety measure is designed with 1oo3 redundancy for the phase 1 accumulator architecture and phase 2

gravity drain lines, along with adoption of direct vessel injection, to ensure single failure tolerance and to minimise reliance on structural integrity arguments for RCS pipework.

There is significant evidence of the application of these processes to demonstrate that the design of SSCs can reduce risks to ALARP; a summary of the evidence is presented in the ALARP Summary Report [3] and within the 'systems engineering' E3S Case chapters. At RD7/DRP1, the evidence focuses on higher safety classified SSCs that are of a higher level of design maturity; however, the overall design approach and evidence to date provides confidence that the design of all SSCs can reduce risks to ALARP.

Further details of how E3S design principles guide and inform the design of SSCs is described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [19].

24.3.4 Defence in Depth

The provision of multiple, independent barriers to provide defence in depth against the progression of fault sequences is a key deterministic safety approach to support reduction of risks to ALARP. Defence in depth against postulated initiating events (PIEs) is achieved by the provision of several consecutive and reasonably practicably independent measures that would have to fail before harmful effects could be caused to people or to the environment. The five levels of defence in depth are described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [19].

For RR SMR, safety measures are employed across all five levels of defence in depth, which are designed to minimise susceptibility to failures on one level affecting any other level. This is achieved using different equipment where reasonably practicable and ensuring that safety functions are delivered diversly from one another such that common causes of failure across multiple safety measures and defence in depth levels are minimised.

The RR SMR safety measure design approach applies a combination of both passive and active safety measures. Overall emphasis is placed on passive safety measures with active safety measures providing diverse defence in depth. Further, diversity is also provided between the various passive safety measures and active safety measures.

The RR SMR fault schedule identifies the safety measures required to provide each of the fundamental safety functions (FSF) [19] in response to faults, across all levels of defence in depth. For example, to provide the FSF of control of fuel temperature (CoFT), the following sequential measures are claimed for many in-tact circuit faults (ICFs) during operating modes 1 and 2:

1. Condenser Decay Heat Removal (CDHR) – duty measure, defence in depth level 1
2. Active Steam Generator (SG) Atmospheric Steam Dumping – preventive measure, defence in depth level 2
3. Passive Decay Heat Removal (PDHR) [JN02] – protective measure, defence in depth level 3
4. Emergency Core Cooling (ECC) [JN01] – protective measure, defence in depth level 3
5. In-Vessel Retention (IVR) – mitigating measure, defence in depth level 4
6. Emergency response procedures – mitigating measure, defence in depth level 5.

The RR SMR is designed to provide at least two independent and diverse safety measures for frequent initiating events (>1E-03 per year) at defence in depth level 3. This is in keeping with UK practice and goes beyond the international practice described by the IAEA, which typically expects provision of at least one safety measure, and then additional 'features' that deliver diversification within the single safety measure rather than requiring a dedicated and separate safety measure.

The PDHR [JN02] and the ECC [JN01] are independent and functionally diverse means of providing the FSF of CoFT in response to faults (as described in the list above). For the FSF of control of reactivity (CoR), the RR SMR has provision of Scram [JD01] and the Alternative Shutdown Function (ASF) [JD02], which provide two functionally diverse means of shutting and holding down the reactor in response to faults, through solid control rods and soluble potassium tetraborate injection respectively. The Containment Safety Measure (CSM) [JM01] provides the FSF of confinement of radioactive material (CoRM), within which the Containment System [JMA] and containment isolation valves provide the function; where two valves are required to provide containment isolation, each valve is reliably and independently actuated.

Most of the SSCs that deliver the PDHR [JN02] and ECC [JN01] safety functions are independent and diverse from each other, however, there are several key items of SSC that are shared. This includes a shared ultimate heatsink, the LUHS [JNK]. The PDHR [JN02] takes steam generated in the steam generators and condenses it inside the Passive Steam Condensing System (PSCS) [JNB] heat exchanger tubes, that are submerged directly in the LUHS [JNK] coupled tank, whilst ECC [JN01] takes steam generated within containment and condenses it on the external surface of the Passive Containment Cooling (PCC) heat exchanger tubes, that are cooled by a natural circulation flow from/to the LUHS [JNK] coupled tank. Multiple options for heatsinks have been evaluated, which concluded that a shared LUHS [JNK] with 1oo3 redundancy (for 24 hours of heat removal, 2oo3 for 72 hours of heat removal) is consistent with UK and international RGP, meets deterministic principles, and is highly reliable such that numerical targets can be met. An additional independent heatsink would only provide a minimal reduction in overall risk, whilst significantly increasing the RR SMR footprint and the height of the hazard shield, therefore the evaluation concludes that the safety benefits from an additional dedicated LUHS [JNK] are grossly disproportionate to the costs of such a design.

The Refuelling Pool [FAF] is also shared between the PDHR [JN02] and ECC [JN01]; the High Pressure Injection System (HPIS) [JND] draws water from the Refuelling Pool [FAF] in support of PDHR [JN02], whilst the ECC [JN01] requires the Refuelling Pool [FAF] inventory to drain into the containment sump to support reactor heat removal. The Refuelling Pool [FAF] is a massive and passive structure with high reliability claims on its structural integrity, and addition of another water source within containment would significantly increase layout complexity and number of components.

The principle of defence in depth is also adopted within the supporting EC&I systems to ensure safety measures can deliver their functions in the event of faults. The electrical systems include:

- Main Grid Connection [AC_] – defence in depth level 1
- The Generator [MKA], Standby Grid Connection [AC_], High Voltage Main AC Supply System [BB_] and the High Voltage Main AC Standby Supply System [BC_] – defence in depth level 2
- High Voltage Essential AC Standby Supply System [BD_] and associated sub-systems, Low Voltage Essential AC Standby Supply System [BK_], Low Voltage Uninterruptible DC Supply System for Safety Services [BQ_] – defence in depth level 3

- Low Voltage Essential AC Alternate Supply System [BL_] – defence in depth level 4
- Mobile power supplies are anticipated at defence in depth level 5 in line with RGP and E3S design principles.

The number of divisions at each level of defence in depth aligns with the trains of process systems and divisions of the control & instrumentation (C&I) systems. The C&I architecture has been developed to align with the defence in depth levels in the fault schedule, allowing for the allocation of safety functions to different systems based on fault schedule allocation to safety measures. This comprises:

- Reactor Control System (RCS) [JSA10], Control Rod Control System (CRCS) [JSA30], Nuclear Heating, Ventilation, Air Condition (HVAC) Supervisory Control System [JSA40], Reactor Plant Monitoring System (RPMS) [JSS], Fuel Route C&I [FY], and Radioactive Waste C&I [KY] – defence in depth level 1
- Reactor Limitation & Preventive Protection System (RLPPS) [JSA20] and CRCS [JSA30] – defence in depth level 2
- Reactor Protection System (RPS) [JRA], Diverse Protection System (DPS) [JQA], and Post-Accident Management System (PAMS) – defence in depth level 3
- SAMS [JRQ20] – defence in depth level 4
- Human machine interfaces (HMI) in the main control room (MCR) and emergency control centre (ECC) – defence in depth level 5.

The provision of both a hardwired DPS [JQA] and an independent and diverse software based RPS [JRA] to perform all safety category A functions provides significant defence in depth to protect against frequent faults and meets UK RGP. This architecture also ensures that safety class 1 protection systems employ diversity in their detection of and response to fault conditions. There is also significant redundancy within each of the safety class 1 (four divisions) and 2 systems (three divisions).

Furthermore, the HVAC [KL] and its supporting Chilled Water System [KJ] are being designed in accordance with independent and diverse defence in depth requirements (as outlined in section 24.3.3), to ensure they do not undermine the independence of safety measures. The design development to achieve this will be presented in Version 3 of the E3S Case.

Overall, at RD7/DRP1 the RR SMR demonstrates significant defence in depth such that risks can be reduced to ALARP, with independent and diverse safety measures available to deliver all FSFs, and enhanced defence in depth through the provision of two independent and diverse measures for frequent faults. Safety measures are also designed with significant levels of redundancy and diversity within them to ensure they are highly reliable in the delivery of their safety functions.

24.3.5 Inherent Safety and Passivity

Central to the RR SMR safety measure design approach are 'passive' safety measures, in line with E3S design principles for a simple and forgiving design and the application of the hierarchy of controls, described section 24.3.3. The IAEA describes passive systems as those that 'take advantage of natural forces or phenomena such as gravity, pressure differences or natural heat convection'.

The RR SMR safety measure design approach applies a combination of both passive and active safety measures; overall emphasis is placed on the design of passive safety measures, with active safety measures providing diverse defence in depth.

For the key safety measures providing the FSF of CoFT (described in section 24.3.4), the ECC [JN01], PDHR [JN02] and IVR all provide passive decay heat removal, noting PDHR [JN02] contains some active elements to enable pressure and inventory control using the HPIS [JND]. CoFT on other levels of depth is provided through active means.

For the key safety measures providing the FSF of CoR, the Scram [JD01] safety measure provides the primary passive means of shutting down the reactor, whilst the diverse ASF [JD02] provides the secondary active means.

The simple and passive nature of the key RR SMR safety measures delivering safety category A and B functions increases the overall reliability and reduces the maintenance burden compared to more complex active safety measures. This supports the demonstration that risks can be reduced to ALARP.

24.3.6 Innovative Design Features

The RR SMR is generally based on established technology and industry practices using RGP and OPEX. Some areas of novelty are adopted with a view of improving safety and reducing risks to ALARP, described in [3]. Key areas of innovation are summarised below.

24.3.6.1 Chemistry

Boron-free Chemistry

All extant commercial pressurised water reactors operate with boric acid dissolved in the reactor coolant as a duty means of controlling core reactivity. The RR SMR operates without maintaining a concentration of soluble boron dissolved in the reactor coolant, with the shutdown margin and hold down achieved by the control rods alone.

An evaluation of the advantages and disadvantages of boron vs boron-free reactivity control is presented in [3], including review of RGP and OPEX, and impact on hazards and faults. The key safety benefits of the boron-free reactivity control include:

- It avoids concerns with boric acid induced corrosion of pressure vessels, bolting and other critical components in the event of a RCS leak.
- It simplifies the plant operation and maintenance by eliminating dilution operations and permits harmonisation of systems/volume chemistries across the reactor.

- It enables the desired pH to be maintained throughout the cycle with a lower volume of pH raising chemical needed.
- It removes the potential for several possible accidents associated with control of reactivity to occur, e.g. unintended boron dilution accidents.
- It maintains a large negative moderator temperature coefficient at all times.
- It reduces authorisation burden, should boric acid and boron salts be banned through Registration, Evaluation, Authorisation and Restriction of Chemicals (REACh), or similar regulation. Numerous boron components are already included on the Substances of Very High Concern list within REACh.
- It reduces environmental discharges, radioactive waste volumes and water processing requirements due to the elimination of boron recycle operations.

Conversely, borated designs require comparatively fewer control rods and control rod drive mechanisms (CRDMs), which decreases the number of head penetrations and therefore potential leak locations resulting in loss of coolant accidents (LOCAs). Furthermore, the addition of soluble boron to the reactor during head lift provides a functionally diverse method of ensuring sub-criticality for the RPV head lift operation, with soluble boron and prevention of rod withdrawal each preventing an unacceptable reactivity addition, whereas boron-free option is reliant on detecting if there is a fault which prevents rods remaining in the core.

Clearly, the use of boron can be demonstrated to be RGP for PWRs and therefore is a well understood and developed solution. The boron free approach adheres to RGP including application of the hierarchy of controls, such as elimination of tritium discharges and generation of tritium, use of passive techniques for safety measures, and reactivity control within boiling water reactors (BWRs).

The evaluation of options concludes that both boron and boron-free designs can reduce risks to levels that are acceptable. RR SMR has selected boron-free reactivity control given the potential additional safety benefits, conditional upon verification and validation (V&V) to qualify the potassium hydroxide chemistry regime (see E3S Case Version 2, Tier 1, Chapter 20: Chemistry [20]), further development of fuel route faults to confirm successful application of the double contingency approach (DCA) for criticality safety (see E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [21]), and confirmatory analysis of the reactor assembly design to achieve its safety functions (see E3S Case Version 2, Tier 1, Chapter 4: Reactor (Fuel and Core) [22]). Whilst this work is ongoing, at RD7/DRP1, it is concluded that boron-free reactivity control can reduce risks to ALARP as the design develops through detailed design.

Potassium Chemistry

RR SMR uses potassium hydroxide as a pH raiser in conjunction with boron-free reactivity control, instead of lithium hydroxide, which is commonly used in PWRs.

There is a vast amount of OPEX available for lithium hydroxide to demonstrate its capability of maintaining a constant pH within the primary circuit of a PWR. There is also OPEX for use of potassium hydroxide, as water-water energy reactors (VVERs) have used potassium hydroxide as a pH raiser in primary coolant water without a reported deleterious effect on reactor coolant system components.

There are advantages of using potassium hydroxide. Neutron reactions with lithium are the second largest contributor to tritium production, hence, selecting a soluble boron-free and potassium chemistry regime removes the two largest contributors to tritium production. Other advantages include a lower cost price and increased availability (in the UK and globally) compared to lithium.

At RD7/DRP1, it is predicted that potassium hydroxide corrosion performance is at least comparable to lithium hydroxide and most likely to be better. Chemicals and materials test programmes are planned to verify the performance of RCS [JE] materials specifically in a boron-free potassium hydroxide environment.

It is concluded at RD7/DRP1 that use of potassium hydroxide as a pH raiser can reduce risks to ALARP as the design develops through detailed design, subject to outcomes of the test programmes.

24.3.6.2 Base Isolation System

One of the innovative technologies for RR SMR is the implementation of aseismic bearings within a base isolation system, described in E3S Case Version 2, Tier 1, Chapter 9B: Civil Engineering Works and Structures [23].

Base isolation is an application of seismic isolation that reduces the response of a structure to horizontal ground motion through the installation of horizontally flexible and vertically stiff seismic isolators between the superstructure and the substructure. The isolators serve two key functions, to support the gravity loads and to protect the supported structure from the damaging effects of horizontal earthquake shaking. The decoupling of the superstructure from ground motion, reduces the response in the structure that would otherwise occur in buildings with non-base isolated raft foundations.

An evaluation of the advantages and disadvantages of raft foundations utilising base isolation against traditional reinforced concrete foundations is presented in [3], including a review of RGP and OPEX for the application of base isolation technology. Learning and RGP for base isolation from six existing PWRs, and two ongoing nuclear construction projects, which utilise seismic isolation devices is informing the RR SMR design at RD7/DRP1, including:

- The preliminary identification of a preferred isolator type (low damping rubber elastomeric bearings).
- The material specification of the bearing to avoid significant ageing effects.
- The inclusion of a moat cap to protect the bearings.
- The height of the supporting pedestals to facilitate through-life EMIT.

The use of RGP and OPEX from similar applications to inform the design of base isolation is a central part of the ALARP demonstration, as described in section 24.2.2, therefore this provides confidence that risks can be reduced to ALARP as it progresses through detailed design and further analysis is undertaken.

24.3.6.3 Emergency Blowdown

The ECC [JN01] uses an innovative Emergency Blowdown (EBD) valve that is passively demanded open on being exposed to certain plant conditions, providing necessary depressurisation for ECC operation.

Options for passive and active (C&I based) means of achieving automatic depressurisation have been evaluated [3]. The spurious opening of the depressurisation line in normal operation would result in a LOCA, however PSA evaluation against numerical targets demonstrate that the passive EBD valve supports a substantial reduction in spurious line opening frequency and core damage frequency (CDF) contribution from the fault, whilst maintaining Automatic Depressurisation System (ADS) reliability [24]. It also provides functional diversity to protect against spurious depressurisation from C&I actuated valve failures.

Therefore, the innovative development of the passive EBD valve provides a significant safety benefit and supports development of a highly reliable passive safety class 1 safety measure that can reduce risks to ALARP.

Further information on the ECC [JN01] and EBD valve is provided in E3S Case Version 2, Tier 1, Chapter 6: Engineered Safety Features [25].

24.3.6.4 Modularisation and Standardisation

Modularisation is one of the key enablers to ensure build certainty for the RR SMR, and is a key differentiator to traditional, large-scale nuclear. It is the intention for the bulk of the RR SMR plant to be assembled in factories and delivered to site to be installed as a series of modules. Modules must be designed to allow as many complex processes as possible to be completed in the factory, and for the installation to be as simple as possible with as few interfaces as possible.

Extensive research and benchmarking from RGP and OPEX are informing the ongoing RR SMR modularisation philosophy at RD7/DRP1, providing learning for the physical activities, organisational and process aspects of a modularisation approach. This learning includes modular construction techniques being deployed in the nuclear industry for power plants, waste management and submarine applications, as well as modular construction in other non-nuclear industrial applications [26].

The RR SMR modularisation approach minimises risks during manufacture, assembly, installation, and commissioning, with modules designed to achieve E3S requirements and any additional hazards introduced are identified and managed to ALARP. To ensure the design can underpin these claims, the E3S design principles are used to inform the early module design, with iterative E3S analysis through the detailed design placing more refined E3S requirements and constraints onto the module design. The modularisation approach also offers conventional safety benefits, in particular reduction of construction risks through minimisation of activities at the construction site and moving them into a controlled factory environment.

The E3S design principles and requirements feed into the module kit of parts (MKoP), which is a library of standardised components that can be configured and used by the layout team to meet the E3S requirements. The MKoP system is built from components such as frames, barriers, floors, racking systems etc., which are standardised SSCs. As such, there is an iterative design relationship between plant layout (described in 24.3.2), the MKoP, against the relevant E3S requirements.

Standardisation provides potential safety and environmental benefits, such as reducing the number of part types to increase reliability, simplify through-life operations, EMIT and decommissioning activities. Conversely, standardisation has the potential to increase the potential for common cause failures, therefore the standardisation approach for the RR SMR specifies that standardisation must not compromise the E3S Case, which includes requirements for diversity.

Therefore, the modularisation and standardisation philosophy at RD7/DRP1 are suitably informed by RGP, OPEX and E3S design principles/requirements, which is aligned to the key ALARP principles set out in section 24.2.2, to provide confidence that risks can be reduced to ALARP.

Further details of modularisation to achieve build certainty are provided in E3S Case Version 2, Tier 1, Chapter 14: Plant Construction and Commissioning [27].

24.4 Analysis Informed Design

24.4.1 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, as described within the Rolls-Royce SMR Hazard Identification Strategy [28]. Hazard identification studies have been undertaken to inform and develop the design up to RD7/DRP1 and will continue to be undertaken as the design develops through to detailed design. The full list of hazard identification studies and outputs are described in the Hazard Log [29].

The RR SMR fault schedule [30] collates 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 safety categorised functional requirements; the SSCs are then classified based on the highest category function they fulfil. Within the fault schedule, all levels of defence in depth are considered are considered (see section 24.3.4).

Deterministic performance analysis is used to verify the safety categorised functional requirements placed onto SSCs by the fault schedule and provide high confidence in their ability to achieve their safety functions and meet relevant acceptance criteria with suitable margin. Deterministic performance analysis is also used to demonstrate the design meets its non-functional requirements such as single failure tolerance.

At RD7/DRP1, bounding faults and accidents (design basis condition (DBC)-1 to design extension condition (DEC)-B) are modelled to demonstrate that the design can achieve its safety functions; the outputs of the analysis undertaken up to RD7/DRP1 is summarised in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [21]. The deterministic analysis is iterative in nature to inform the evolving design, therefore will continue to develop with a wider set of fault sequences modelled and outputs fed back into the detailed design development. Adoption of the deterministic methods that are RGP and outputs up to RD7/DRP1 provide significant confidence that the design can achieve its safety functions as the design progresses through detailed design,

24.4.2 Probabilistic Safety Assessment

PSA is used to assess the risks associated with design and operation to inform design decision-making, as well as quantification of risks to workers and the public and assessment against numerical risk targets (set out in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [19]) to confirm whether risks are acceptable and ALARP.

PSA has been employed from the early stages of the RR SMR design programme up to RD7/DRP1, with the fault and event tree modelling continuously maturing alongside the design to build confidence that nuclear safety risks posed by the design are below targets, balanced and ALARP.

At RD7/DRP1, the level 1 PSA calculates a CDF of {REDACTED} per year of power operation. This is a factor of {REDACTED) times higher than the RR SMR design target of 1E-07 per year. However, this

result is derived with significant scope limitations and several modelling assumptions that are conservative, such as the attribution of conservative values assigned to operator actions. A complimentary assessment of limitations of the PSA model at RD7/DRP1 provides further commentary and comparison against numerical targets, highlighting further areas of focus and refinement in the ongoing PSA development and scope to present a balanced best estimate risk view.

Nevertheless, the PSA results provide insight and confidence that the RR SMR presents a balanced design. ICFs collectively account for 44 % of plant fault CDF, with loss of electrics faults accounting for 35 %, and LOCA faults accounting for 21 %. However, there is a disproportionate CDF contribution for the event of a LOOP together with failure of house load generation, which is a sequence where the operator fails to maintain diesel generator fuel levels beyond the first 72 hours of LOOP. This sequence's contribution to CDF is 33 %. However, the assessment of limitations identifies an approximately three-decade reduction in frequency from this sequence with conservatisms addressed; namely, crediting non-electrically dependent supply of water to the LUHS [JNK] and re-evaluation of the probabilities assigned to operator error and house load failure.

PSA has informed the design up to RD7/DRP1 through workshop sessions with system designers and formal transmittal of PSA results, with sensitivity studies conducted on various design options and design development to support decision-making and demonstrate that design solutions are contributing to reducing risks to ALARP; these are described in [3]. This includes optimisation for reliability using importance analysis to inform safety measures design, and assurance of dependencies between safety measures.

The use of PSA to inform the design from an early stage and the outputs of the PSA undertaken up to RD7/DRP1, provide confidence that risks are being iteratively assessed against numerical targets and can be reduced to ALARP. The limitations of the PSA model at RD7/DRP1 are understood and documented, with further work defined and understood to refine the model and support risk informed design, such as modelling of hazards and additional operating modes beyond modes 1 and 2, development of level 2 and 3 PSA models, and use of PSA to risk inform EMIT activities and operational limits and conditions (OLCs).

Further evidence of PSA informing design and evaluation against numerical risk targets is summarised in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [21].

24.4.3 Internal Hazards Analysis

The compact RR 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.

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

At RD7/DRP1, the plant has been designed with measures to prevent and protect against hazards, primarily through segregation of safety systems and hazard sources. Based on the inputs, assumptions and results of the analysis, the assessment derives requirements for the civil and modular design of each block in the Reactor Island, including segregation barriers, as well as identifying areas where segregation is not applied, and local protection is required. Evidence of how internal hazards analysis has informed design is summarised in [3].

The internal hazards input to the design up to RD7/DRP1 has set out key principles and methodologies to embed inherent safety within the layout design (see section 24.3.2), and to set out the basis for internal hazard assessments. Assessment of internal hazards sequences and associated safety measures to deliver safety functions are captured within the fault schedule, which will allocate safety categorised functional requirements onto SSCs. The approach to embed internal hazards principles within the layout design provides confidence that the design prioritises inherent safety and will be capable of achieving the requirements set by internal hazards whilst reducing risks to ALARP.

Further evidence of internal hazards informing design is summarised in E3S Case Chapter 15: Safety Analysis [21].

24.4.4 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 to ensure it can withstand external hazards. The effects of climate change over a 100-year period following initial deployment are addressed, covering the design operational life of the RR SMR, potential lifetime extension and estimated decommissioning period.

Following establishment of screened hazards, values have been determined that are relevant to Great Britain (GB). Due to the nature of some external hazards being site dependent, the generic site envelope is conservative to encompass a wide range of potential sites.

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

- Hazard Shield, a reinforced concrete structure providing aircraft impact protection to SSCs which are required to deliver and maintain the plant in a stable, safe state.
- Base isolation system within the hazard shield (see section 24.3.6), comprising a concrete pedestal/plinth, supporting a horizontally flexible and vertically stiff aseismic bearing. The aseismic bearing 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.

Assessment of external hazards sequences and associated safety measures to deliver safety functions are captured within the fault schedule, which will allocate safety categorised functional requirements onto SSCs. The approach to identify external hazards and develop a conservative set of parameters for the RR SMR design provides confidence that the design will be capable of achieving the requirements to withstand external hazards whilst reducing risks to ALARP.

Further evidence of external hazards informing design is summarised in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [21].

24.4.5 Severe Accident Analysis

The RR SMR severe accidents analysis (SAA) provides confidence in the defence in depth level 4 safety measures included in the RR SMR design to prevent an uncontrolled release of radioactive material into the internal or external environment for design extension conditions involving core

melt (DEC-B). This includes the Containment Safety Measure (CSM) [JM01], including IVR and hydrogen reduction system (described in E3S Case Version 2, Tier 1, Chapter 6: Engineered Safety Features [25]).

The SAA identifies severe accident scenarios for analysis through a robust and appropriate means, providing the supporting evidence that the design provisions will maintain safety functions, and that the safety measures are able to deliver their safety requirements. The results of the SAA also provide supporting evidence to the PSA for the development of the plant risk profile.

The iterative nature of the SAA means that the RD7 design has been informed by SAA undertaken on the RD6 design; details of the analysis outputs are summarised in [3]. Overall, the SAA demonstrates that the fundamental power station design successfully mitigates the consequences of a range of limiting severe accidents and no fundamental safety shortfall has been identified. This provides confidence that the RR SMR can reduce risks associated with accidents leading to core melt to ALARP. As the SAA is developed it will continue to inform the CSM [JM01] design to ensure it can achieve is safety requirements and will identify any further measures required to reduce risks to ALARP.

Further evidence of SAA informing design is summarised in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [21].

24.4.6 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.

There are key areas where radiation protection principles have influenced design at RD7/DRP1. These are summarised in the radiation protection ALARP topic report [31], which concludes that at RD7/DRP1 the radiation protection principles implemented during the early design phases are directing the design towards reducing doses to workers and members of the public to ALARP.

The assessment of normal operation doses at RD7/DRP1 is summarised in E3S Case Version 2, Tier 1, Chapter 12: Radiation Protection. The assessment demonstrates that radiation worker doses are below basic safety levels (BSLs), noting the assessment is iterative and used to inform the ongoing design of shielding and other design features to further reduce doses towards basic safety objectives (BSOs). All other worker and public doses are assessed to be well below BSOs.

At RD7/DRP1, it is concluded that there is high confidence that the design will, in all cases, be able to reduce doses to ALARP.

24.4.7 Human Factors Analysis

Human factors (HF) have been integrated within the SMR programme since its early conception, through a programme of HF activities set out in the human factors integration plan (HFIP). Some key analysis and design activities undertaken up to RD7/DRP1 that support reduction of risks to ALARP include:

- A comprehensive review of the PIE definitions and initiating event frequencies has verified the correct allocation of those faults attributed to operator error and provided confidence that the deterministic safety analysis covers all credible faults.

- Operator actions are assessed within the PSA (see section 24.4.2), with several operator actions presenting a significant contribution to risk and the overall CDF. Further development of the PSA and human error probabilities are expected to significantly improve, thus reducing the overall risk.

- Early integration of HF into design is provided through contribution to the hazard identification process to support identification of any potential risks and safeguards.

- The allocation of function has advised only 9 % of functions should be allocated to fully manual (local or remote) tasks, supporting the E3S design principle for systems to be passive or automated.

Further details are provided in [3], which concludes that the continued integration of HF through allocation of function, provision of design guidance and human reliability analysis, provide confidence that the identification of potential operator error can be reduced to ALARP.

24.4.8 Conventional Safety Analysis

The principles of prevention are applied to the RR SMR in line with the hierarchy of controls to ensure that conventional and fire hazards are eliminated wherever practicable before control measures are introduced. This is in line with the regulations which require the demonstration of how risks have first been eliminated before reducing risk to ALARP.

The overarching approach is that conventional and fire legislation and regulations, such as the Construction (Design and Management) Regulations 2015 (CDM), are fully integrated within the RR SMR design management systems, processes, and procedures at RD7/DRP1 (rather than undertaken as auxiliary activities, as can often be the practice).

The RR SMR design for conventional safety process ensures that conventional safety requirements inform the design. The application of this process as the design progresses into detailed design provides confidence that the RR SMR can demonstrate compliance with legislation and regulations to eliminate hazards and reduce conventional and fire risks to ALARP.

24.5 Risk Reduction Through-Life

24.5.1 Construction

The RR SMR approach to construction is described in E3S Case Version 2, Tier 1, Chapter 14: Plant Construction and Commissioning [27]. The ALARP aspects of the modularisation approach are described in section 24.3.6.4 of this chapter.

24.5.2 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.

One of the key commissioning strategies is the opportunity to utilise enhanced factory acceptance testing (FAT) on SSCs constructed within RR SMR modules in the offsite factory, to reduce the activities (e.g., completions, handovers) that need to be carried out in the on-site factory. This builds on, and is enabled by, the project's modularisation philosophy.

Testing in a clean factory environment where specialist equipment is close at hand and systems are easily accessible can provide safety benefits and reduce onsite risks, as well as reducing the schedule of on-site activity.

Further details are outlined in E3S Case Version 2, Tier 1, Chapter 14: Plant Construction and Commissioning [27].

24.5.3 Operations

Operating philosophies are being developed alongside design, and processes being developed to ensure OLCs from the design and E3S 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 Version 2, Tier 1, Chapter 13: Conduct of Operations [32] and E3S Case Version 2, Tier 1, Chapter 16: Operational Limits and Conditions for Safe Operation [33].

24.5.4 Decommissioning

The preferred decommissioning strategy selected for RR SMR is immediate decommissioning, which is consistent with UK Government policy and guidance. 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 principles are developed for RR SMR based on a review of applicable international and national regulations and guidance, which are used to inform the design. Design features that support decommissioning and minimisation of waste are described in [3], including features such as

decay storage of resins/concentrates to reduce intermediate level waste (ILW) volumes, and use of backwashable filters that do not require filter changes and reduce operator maintenance dose.

It is also recognised that the overall RR SMR design provides opportunities to reduce risks during decommissioning, including:

- 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.

- The deployment of multiple RR SMRs 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.

Further information is provided in E3S Case Version 2, Tier 1, Chapter 21: Decommissioning and End of Life Aspects [34].

24.6 Conclusions

24.6.1 Assumptions & Commitments on Future Dutyholder

None identified at this revision.

24.6.2 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' [2]. 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 24 is 'the RR SMR design permits construction, commissioning, operation, maintenance and decommissioning with risks and exposures reduced to ALARP'.

The arguments and evidence presented to meet the generic E3S Case objective at Version 2 include the RR SMR ALARP principles, which broadly cover RGP, design optioneering, risk assessment, and implementation of improvements. These principles are embedded into the E3S and engineering processes, including design optioneering and through progressive and iterative safety analysis, as set out in the E3S Requirements and Analysis Arrangements [15].

At the plant level, the selection of PWR technology for the RR SMR offers a vast amount of RGP and OPEX. The layout is being developed with input from E3S to ensure high levels of inherent safety to eliminate risks. Significant defence in depth is provided through safety measures across all five levels, including enhanced defence in depth through the provision of two independent and diverse measures for protection against frequent faults.

The design of all SSCs is developed in accordance with the systems engineering design process. This includes alignment to RGP and OPEX, design to codes and standards according to their safety classification, and the extensive systematic optioneering process with down-selection of design options based on assessment against relevant E3S criteria. Safety measures are also designed in line with principles for a simple and forgiving design and the application of the hierarchy of controls, increasing reliability, and reducing the maintenance burden.

Innovative design features are adopted with a view of improving safety and reducing risks, including boron-free chemistry, base isolation, EBD for ECC [JN01] operation, and modularisation to enable build certainty. At RD7/DRP1, it is concluded that these design features have the potential for significant safety benefits and risk reduction.

The suite of safety analysis used to inform the design and evaluate risks against numerical criteria includes deterministic, probabilistic, hazards, severe accident, radiation protection, human factors, and conventional and fire analyses. The analysis is iterative in nature and has generally been undertaken on previous reference design baselines to inform the design at RD7/DRP1; the analysis undertaken at this stage provides confidence that the design can achieve numerical targets and reduce risks to ALARP.

In conclusion, the ALARP demonstration at RD7/DRP1 supports the generic E3S Case in achieving its objective 'to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design' [2]. Further

arguments and evidence to underpin the claims in support of this objective will be developed in line with the E3S Case Route Map [4] and reported in future revisions of the generic E3S Case.

24.7 References

[1] Rolls-Royce SMR Limited, SMR0001603 Issue 1, “Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles,” August 2022.

[2] Rolls-Royce SMR Limited, SMR0004294 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction,” May 2024.

[3] Rolls-Royce SMR Limited, SMR0009086 Issue 1, “ALARP Summary Report,” January 2024.

[4] Rolls-Royce SMR Limited, SMR0002155 Issue 3, “E3S Case Route Map,” November 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] Office for Nuclear Regulation, NS-TAST-GD-005 Issue 12, “Regulating duties to reduce risks to ALARP,” January 2024.

[8] 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].

[9] IAEA, “Fundamental Safety Principles,” 2006.

[10] WENRA, “Safety Reference Levels for existing Reactors,” 2014.

[11] Health and Safety Executive, “Ionising Radiation Regulations,” 2017.

[12] Industry Radiological Protection Co-Ordination Group, “The Application of ALARP to Radiological Risk: A Nuclear Industry Good Practice Guide,” 2012.

[13] Rolls-Royce SMR Limited, TS-DD-02, “Decision Record Template”.

[14] Rolls-Royce SMR Limited, 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].

[15] Rolls-Royce SMR Limited, SMR0009132 Issue 1, Environment, Safety, Security and Safeguards (E3S) Requirements and Analysis Arrangements, 2023.

[16] Rolls-Royce SMR, SMR0007298 Issue 1, “Reactor Island Architectural and Layout Summary Report,” January 2024.

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

[18] Rolls-Royce SMR Limited, C3.1.1, Define and Manage Requirements, April 2023.

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

[20] Rolls-Royce SMR Limited, SMR0004982 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 20: Chemistry,” May 2024.

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

[22] Rolls-Royce SMR Limited, SMR0004210 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 4: Reactor (Fuel and Core),” May 2024.

[23] Rolls-Royce SMR Limited, SMR0003778 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 9B: Civil Engineering Works and Structures,” May 2024.

[24] Rolls-Royce SMR Limited, EDNS01000537027/001, “SMR Probabilistic Safety Assessment,” March 2021.

[25] Rolls-Royce SMR Limited, SMR0003771 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 6: Engineered Safety Features,” May 2024.

[26] Rolls-Royce SMR Limited, SMR0008962 Issue 2, “Modular Kit of Parts Strategy,” January 2024.

[27] Rolls-Royce SMR Limited. SMR0004289 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 14: Plant Construction and Commissioning,” May 2024.

[28] Rolls-Royce SMR Limited, SMR0001228 Issue 2, “Rolls-Royce SMR Hazard Identification Strategy,” July 2023.

[29] Rolls-Royce SMR Limited, SMR0001317 Issue 4, “Rolls-Royce SMR Hazard Log Report - Version 7,” January 2024.

[30] Rolls-Royce SMR Limited, SMR0004444 Issue 3, “Rolls-Royce SMR Fault Schedule (Version 7),” January 2024.

[31] Rolls-Royce SMR Limited, SMR0007303 Issue 1, “Radiation Protection ALARP Topic Report,” January 2024.

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

[33] Rolls-Royce SMR Limited, SMR0004555 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 16: Operational Limits and Conditions for Safe Operation,” May 2024.

[34] Rolls-Royce SMR Limited, SMR0004599 Issue 3, “Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 21: Decommissioning and End of Life Aspects,” May 2024.

24.8 Appendix A: Claims, Arguments, Evidence

Table 24.8-1 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. 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 [2].

Table 24.8-1: Mapping of Claims to Chapter Sections

Claim	**Section of Chapter 24 containing arguments / evidence summary**
The RR SMR ALARP methodology reflects RGP and is embedded into the engineering processes, to ensure the design is optimised to reduce risks to ALARP	24.2
The fundamental reactor design is based on a proven and safe PWR technology	24.3.1
Overall site layout is optimised to reduces risk to ALARP through-life	24.3.2
SSC design reduces risks to ALARP through-life	24.3.3
Novel design aspects are well understood, justified, and reduce risks to ALARP	24.3.6
Design adopts inherent protection, design simplicity, and passive safety measures, where practicable	24.3.5
Safety Measures across defence in depth level are independent, or where independence is not practicable, the associated risks are justified and ALARP	24.3.4
Independent safety measures are protected against common cause failures through provision of redundancy, diversity and segregation	24.3.3
The design provides multiple independent, physical barriers to ensure confinement of radioactive material	24.3.4
All reasonably practicable measures are implemented across the design	24.4.2
Deterministic safety analysis has informed the design to reduce risks to ALARP	24.4.1
Probabilistic safety assessment has informed the design to reduce risks to ALARP	24.4.2
Internal Hazards analysis has informed the design to reduce risks to ALARP	24.4.3
External Hazards analysis has informed the design to reduce risks to ALARP	24.4.4

Claim	**Section of Chapter 24 containing arguments / evidence summary**
Severe accident analysis has informed the design to reduce risks ALARP	24.4.5
Radiological assessment has informed the design and exposures are reduced to ALARP	24.4.6
Conventional Safety assessment has informed the RR SMR design to reduce risks to ALARP	24.4.8
Human Factors is integrated into the design to reduce risks to humans to ALARP	24.4.7
Approach for commissioning of SSCs reduces risks to ALARP	24.5.2
Arrangements for operations and maintenance, including definition of Operational Limits and Conditions, reduce risks to ALARP	24.5.3
Decommissioning strategies reduce risks to ALARP	24.5.4

24.9 Abbreviations

ADS	Automatic Depressurisation System
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
ASF	Alternative Shutdown Function
BAT	Best Available Techniques
BSL	Basic Safety Level
BSO	Basic Safety Objective
BWRs	Boiling Water Reactor
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CDF	Core Damage Frequency
CDHR	Condenser Decay Heat Removal
CDM	Construction (Design and Management) Regulations 2015
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRM	Confinement of Radioactive Material
CRCS	Control Rod Control System
CRDM	Control Rod Drive Mechanism
CSM	Containment Safety Measure
DBC	Design Basis Condition
DCA	Double Contingency Approach
DEC	Design Extension Condition
DPS	Diverse Protection System
DRP	Design Reference Point
E3S	Environment, Safety, Security and Safeguards
EBD	Emergency Blowdown
EC&I	Electrical, Control and Instrumentation
ECC	Emergency Core Cooling
EMIT	Examination, Maintenance, Inspection and Testing

FAT	Factory Acceptance Testing
FSF	Fundamental Safety Function
GB	Great Britain
GDA	Generic Design Assessment
HF	Human Factors
HFIP	Human Factors Integration Plan
HMI	Human Machine Interface
HPIS	High Pressure Injection System
HVAC	Heating, Ventilation, Air Conditioning
IAEA	International Atomic Energy Agency
ICFs	Intact Circuit Faults
ILW	Intermediate Level Waste
IVR	In-Vessel Retention
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-site Power
LUHS	Local Ultimate Heat Sink
MCR	Main Control Room
MKoP	Modular Kit of Parts
NRC	Nuclear Regulatory Commission
OLC	Operational Limit and Condition
ONR	Office for Nuclear Regulation
OPEX	Operating Experience
PAMS	Post-Accident Management System
PCC	Passive Containment Cooling
PDHR	Passive Decay Heat Removal
PIE	Postulated Initiating Events
PSA	Probabilistic Safety Assessment
PSCS	Passive Steam Condensing System

PWR	Pressurised Water Reactor
R2P2	Reducing Risks, Protecting People
RCA	Radiation Controlled Areas
RCS	Reactor Coolant System
RD	Reference Design
REACh	Registration, Evaluation, Authorisation and Restriction of Chemicals
RGP	Relevant Good Practice
RLPPS	Reactor Limitation & Preventive Protection System
RPMS	Reactor Plant Monitoring System
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RR SMR	Rolls-Royce Small Modular Reactor
SAA	Severe Accidents Analysis
SAPs	Safety Assessment Principles
SFAIRP	So Far As Is Reasonably Practicable
SG	Steam Generator
SSC	Structure, System and Component
UK	United Kingdom
V&V	Verification & Validation
VVER	Water-Water Energy Reactor
WENRA	Western European Nuclear Regulators Association
WNA	World Nuclear Association