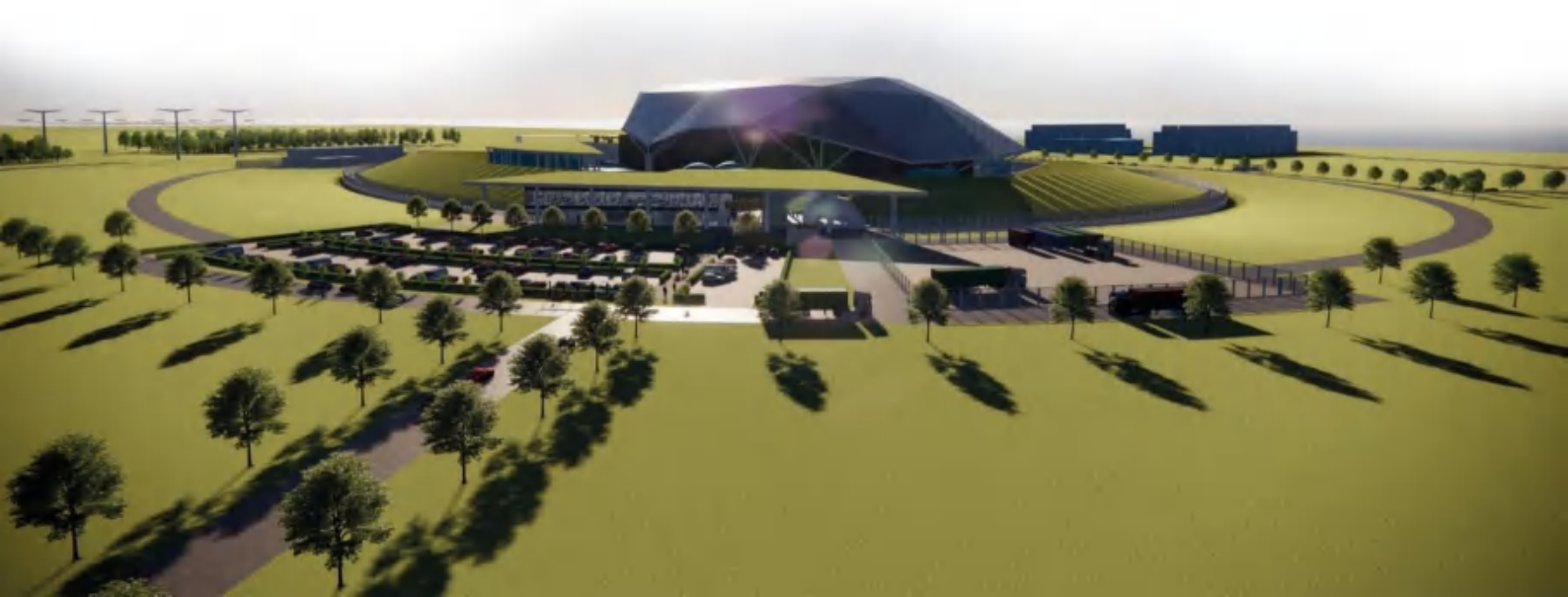
Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 24: ALARP Summary



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 Minor template/editorial updates for overall E3S Case consistency.
August 2025	4	Issue	Updated for Version 3 of the E3S Case. Supports and incorporates revisions at Design Reference Point 4. Chapter changes include: • Narrative on Route Map added (24.0.3) • Further clarity on steps of the ALARP methodology and how it is implemented (24.1.2) • Updated arguments for layout risk reduction (24.2.2) • Updated information on how SSC design reduces risks (24.2.3) • Updated information on the implementation of Defence in Depth (24.2.4) • Addition of Spent Fuel Pool measure passivity (24.2.5) • Enhanced ALARP arguments for novel design features (24.2.6) • Updated outputs of analysis and associated ALARP arguments (24.3) • Minor clarifications to through-life risk reduction (24.4) • Enhanced conclusions on ALARP position (24.5)

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. Version 3 of the generic E3S Case is developed in support of the Design Reference Point 4 (DRP4).

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 Pressurised Water Reactor (PWR) technology for the RR SMR offers access to a vast amount of RGP and Operating Experience (OPEX). The layout is 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 (HF), and conventional and fire analyses. The analysis concludes that the design is capable of achieving numerical targets and can reduce risks to ALARP, and further confirmatory analysis will be presented to build on this confidence as the detailed design progresses.

Contents

24.0 Introduction to Chapter

24.0.1 Introduction

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 Version 3 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 through 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 progresses through detailed design.

24.0.2 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 holistic ALARP demonstration for the entire RR SMR design and lifecycle. Reference is made to relevant Tier 1 chapters and Tier 2 documents of the E3S Case where more specific or detailed arguments and evidence are presented.

Version 3 of the generic E3S Case is based on Design Reference Point 4 (DRP4). Given the iterative nature of the E3S analysis alongside the maturing design, the safety analysis described within this chapter are generally based on an earlier design baseline that has informed DRP4. The relevant design reference is stated within the relevant sections for each safety analysis discipline.

The chapter provides confidence that the design is capable of reducing risks to ALARP as it is developed through detailed design and does not (and cannot at this stage) present a 'final' ALARP position. This reflects the objective of Version 3 of the generic E3S Case, as stated in E3S Case Tier 1 Chapter 1: Introduction [2].

24.0.3 Claims, Arguments and Evidence Route Map

The E3S Case employs a Claims, Arguments, Evidence (CAE) framework to provide a structured demonstration that the RR SMR achieves the E3S fundamental objective 'to protect people and the environment from harm' through compliance with the E3S design principles, as described in E3S Case Tier 1, Chapter 1: Introduction [2]. The CAE framework is presented in the E3S Case Route Map [3].

The claims decomposition for Chapter 24 is developed from the Chapter 3 claim that 'The design reduces risks and exposures to ALARP', which is further decomposed into sub-claims described below.

This chapter presents a holistic ALARP position for Version 3 of the generic E3S Case, with focus on the summarising the overarching arguments and evidence that underpin the claims being made. It draws upon information from across all Tier 1 chapters of the case. Further information to support the ALARP position is presented in the ALARP Summary Report [4], which pulls together and

provides detailed commentary on the significant suite of evidence from lower tier design decision records and safety analysis documents.

[Sub-Claim 24.1] The design incorporates Relevant Good Practice and Operating Experience.

Arguments and evidence to underpin the claim is summarised in:

- Section 24.1.2, which summarises how RGP and OPEX are considered, incorporated and evidenced through the design processes.
- Section 24.2, which summarises how RGP and OPEX have informed the key design aspects for RR SMR. Section 24.2.6 presents the ALARP arguments for novel aspects of the design where RGP and OPEX may not be readily available.

[Sub-Claim 24.2] Design options are evaluated against E3S criteria to reach an optimised design solution.

Arguments and evidence to underpin the claim is summarised in Section 24.2.3, which summarises how the design of all SSCs is optimised and evaluated through the integrated E3S and engineering processes.

[Sub-Claim 24.3] Risks are assessed and drive safety improvements.

Arguments and evidence to underpin the claim is summarised in:

- Section 24.1.2, which summarises how the safety analysis is used to iteratively inform the design.
- Section 24.3, which summarises the key insights and conclusions from the safety analysis that have informed the design.

[Sub-Claim 24.4] No further reasonably practicable safety improvements can be implemented.

Given the nature of the maturing design and analysis at DRP4, definitive conclusions that no further measures can be implemented are not made. More appropriately, confidence statements on the ALARP position at DRP4 for how risks are capable of being reduced to ALARP are presented through this chapter and the conclusions in Section 24.5.

24.0.4 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 (IAEA), 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].

24.1 ALARP in Decision Making Process

24.1.1 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 IAEA, United States Nuclear Regulatory Commission (US 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.

24.1.2 Methodology

24.1.2.1 ALARP Principles

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 the suite of safety analysis undertaken to inform the design. As such, the principles of ALARP have been inherent to the design development programme to drive safety improvements into the design from the outset of the project, aiming to minimise the need to 'retrofit' ALARP improvements at a later stage.

Further information on the ALARP principles is presented in the ALARP Summary Report [4].

24.1.2.2 Relevant Good Practice

RGP is fundamentally embedded into the E3S design principles [1], which provide the framework against which the RR SMR is developed and evaluated. The E3S design principles are derived and

justified based on an extensive review of UK and international practices for nuclear facilities, including the IAEA suite of guidance for nuclear power plant design, WENRA safety reference levels and guidance, European Utility Requirements (EUR), ONR SAPs and Security Assessment Principles (SyAPs), and Environment Agency (EA) Regulatory Guidance.

RGP incorporated into the principles covers the design development, for example design simplicity and preference to eliminate risks over controlling them. It also covers analysis methods, for example establishing suitable numerical targets for evaluation of risks and doses.

Within the design development processes, the study of RGP and Operating Experience (OPEX) is central to optioneering studies, described below.

24.1.2.3 Optioneering

The conduct design optioneering process [13] includes the 20 key design objectives and criteria against which the design options are evaluated. 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.

The evaluation of options includes a comprehensive review of RGP and OPEX, and an assessment of risk against more detailed E3S criteria, such as their impact on fault and hazard sequences, probabilistic safety targets, conventional health and safety, Human Factors (HF), and radiological dose. E3S stakeholders support this risk evaluation and decision analysis to inform down-selection of design solution(s).

The outputs of the optioneering studies are recorded within the decision record template [14], which captures the evaluation evidence for why the design solution(s) reduces risks to ALARP (and uses BAT and is secure/safeguards by design). The decision record is a key Tier 3 evidence document for the E3S Case. All design decisions are listed in the RR SMR Decision Register [15].

Within Tier 1 of the E3S Case, key decisions with respect to ALARP are highlighted within the SSC descriptions in the systems engineering chapters 4 to 11.

24.1.2.4 Risk Assessment

Risk is continuously assessed through progressive and iterative safety analysis, as set out in the E3S Requirements and Analysis Arrangements [16] and the supporting suite of Standards. This process may lead to revisiting optioneering decisions and design iteration to support the demonstration of ALARP through detailed design.

The safety analysis used to support a decision is captured within the decision record template [14]. The holistic analysis for each discipline, including assessment against numerical targets, is summarised in the relevant Tier 1 chapters, including E3S Case Tier 1, Chapter 12: Radiation Protection [17], E3S Case Tier 1 Chapter 15: Safety Analysis [18]), E3S Case Tier 1, Chapter 18: Human Factors Engineering [19], and E3S Case Chapter Tier 1, Chapter 22: Conventional & Fire Safety [20].

24.1.2.5 Conclusion on Further Improvements

Version 3 of the E3S Case does not conclude that ‘no further reasonably practicable improvements can be made’, given that the detailed design is ongoing and iterative safety analysis may lead to design iteration to support risk reduction to ALARP. However, ALARP principles are embedded through the design processes to ensure risk reduction to ALARP is considered from early in the design development, with further analysis informed design enhancement developing the strong base position. As such, confidence statements are made throughout the E3S Case that the design and analysis up to DRP4 demonstrate that risks are capable of being reduced to ALARP. This chapter

and the supporting Tier 2 ALARP Summary Report [4] provide an overall conclusion on this ALARP position at DRP4.

24.1.3 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 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.

24.2 Key Design Aspects

24.2.1 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 draws upon a vast amount of OPEX in designing, manufacturing, installing, testing, commissioning, maintaining and refurbishing PWRs (see E3S Case Tier 1, Chapter 1: Introduction [2]).

In the early stages of the RR SMR development, the fundamental configuration of the Reactor Coolant System (RCS) [JE] was subject to optioneering, with two, three and four loop options evaluated. The three-loop RCS [JE] 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 [JE] configurations with more loops, whilst providing safety benefits through increased redundancy over RCS [JE] configurations with fewer loops.

The use of RGP is key to the ALARP demonstration, 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.

24.2.2 Layout

The RR SMR site and plant layout are being designed to reduce risks during normal operation, faulted operation and accident conditions, at all stages of the lifecycle. To achieve this, E3S design principles are applied to the plant layout, described in E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21]. These principles are decomposed into a more detailed set of E3S requirements and constraints, covering all aspects of E3S including (but not limited to) Internal Hazards (IHs), External Hazards (EHs), conventional safety, radiation protection, and HF.

The E3S requirements and constraints are implemented into the layout as part of the layout design process. This is iterative as the E3S analysis is performed on the maturing layout, which results in further refinement of the layout against the E3S requirements. This approach promotes elimination of risks in accordance with the hierarchy of controls and reduces the need to 'back-fit' measures to control risks at a later stage when the detailed layout has been 'finalised'. Examples of how the E3S design principles, requirements and constraints are considered within the layout design are presented in the Reactor Island Architectural and Layout Summary Report [22], noting this report reflects a previous layout design reference and is being revised and expanded to each Reactor Island block for Version 4 of the generic E3S Case.

Key design features of the layout to reduce risks at DRP4 include, but are not limited to:

- Spatial separation of trains and barrier segregation/compartmentalisation through fire barriers, of highly safety classified SSCs to ensure safety functions can be achieved following IHs. This applies to the mechanical systems and the supporting electrical and Control & Instrumentation (C&I) systems that may be required to deliver the safety functions, including the Diesel Generators (DGs) and the Reactor Protection System (RPS) [JRA].
- Locating buildings containing highly safety classified SSCs within the Hazard Shield and on the Seismic Isolation System (SIS) to attenuate loads and ensure safety functions can be achieved following EHs. The exceptions are the Essential Service Water System (ESWS)

[PB] trains and Back-up Generation System (BUGS) [UBM] containing the DGs, which are instead protected by independent redundancy and separation, with their respective duplicate trains being situated North and South of the Hazard Shield structure.

- Escape routes with maximum distances in accordance with conventional safety and fire standards.
- Design of access routes in accordance with the HF Target Audience Description (TAD), such as minimum passageway and stair widths.
- Radiation shielding integrated into the layout by means of a combination of civil structures and Modular Kit of Parts (MKoP) barriers, to minimise individual and collective dose to ALARP.
- Clear delineation of Radiation Controlled Areas (RCA) and non-RCA, with the health physics laboratory on the main personnel route into the RCA, to minimise radiation exposures to workers.
- Allocation of adequate spacing to enable replacement of components during plant life, for example placement of large heat exchangers in the safety fluids block, and for Examination, Maintenance, Inspection and Testing (EMIT) activities, noting appropriate assumptions are made where EMIT activities are not yet fully defined.

The layout design approach also provides the opportunity to evaluate competing E3S requirements (and non-E3S requirements such as constructability) through the design optioneering process to make risk-informed decisions and optimise the layout as necessary. As such, the layout is designed to reduce risks at a holistic level not for individual areas in isolation. For example, the layout decision for a linear configuration of the Spent Fuel Pool (SFP) [FAB10], Upender Pit [FAB40], and Cask Loading Pit within the Fuelling Block has been reached following evaluation of advantages and disadvantages with respect to E3S [23]. The evaluation recognises the safety benefits, such as the Fuel Transfer Channel (FTC) gate valve being recessed into the wall structure in accordance with RGP, and reduction in overall Fuel Handling Machine (FHM) movements to reduce potential for collisions and dropped loads. The decision-making is balanced against potential sustainability disadvantages such as an increased SFP [FAB10] volume and hence concrete volume for the pool and pit structures, noting this is offset by the overall decrease in Reactor Island footprint and minimisation of build and materials used.

By its nature, the RR SMR has a smaller footprint compared to traditional large-scale nuclear plants, where a larger site offers advantages such as IH tolerance by virtue of larger physical distances for segregation of redundant trains of safety measures, or EMIT benefits through larger laydown and outage spaces for people and equipment. However, the E3S design principles drive the RR SMR to provide equivalent or enhanced levels of safety without reliance on larger distances, achieved through the implementation of E3S requirements and constraints into the layout. This, for example, results in greater emphasis on physical barriers to achieve segregation requirements for IH protection.

The E3S analysis presented across the E3S Case provides supporting evidence to underpin claims that the layout supports risk reduction. For example, the IH analysis presented in E3S Case Tier 1 Chapter 15: Safety Analysis [18] and shielding/dose rate assessments presented in E3S Case Tier 1, Chapter 12: Radiation Protection [17], support the demonstration of tolerance to IHs and reduction of doses to below numerical targets (and to ALARP).

The layout design overview at DRP4 is summarised in the Reactor Island RD9 Readiness Review [24]. This has been optimised from previous layout designs to improve build certainty aspects. The evaluation of E3S and ALARP aspects (and BAT, secure/safeguards/sustainability by design) is captured within a series of supporting design decision records, which provide confidence that risks

for the DRP4 layout design remain capable of being reduced to ALARP. Iteration of the E3S analysis is planned for the DRP4 layout, which is anticipated to inform further layout optimisation through detailed design such that a robust ALARP demonstration can be developed in future iterations of the case.

24.2.3 SSC Design

SSCs are matured through a formalised gated review process and are designed in accordance with integrated E3S and engineering processes. The design process incorporates extensive optioneering, including incorporation of RGP and OPEX and down-selection of design options based on assessment against relevant E3S criteria, as described in Section 24.1.2. This ensures the ongoing design of SSCs drive risk reduction to ALARP, as well as demonstrating BAT and secure/safeguards by design.

SSCs are fundamentally designed to achieve E3S functions, including Fundamental Safety Functions (FSFs), Fundamental Environment Functions, cyber and physical security functions, and safeguards functions, as described in E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21]. The FSFs include Control of Reactivity (CoR), Control of Fuel Temperature (CoFT), Confinement of Radioactive Material (CoRM), and Control of Radiation Exposure (CoRE).

E3S functions are allocated to measures, and SSCs that comprise them, through the application of E3S Requirements and Analysis Arrangements [16]. E3S functions are categorised in accordance with E3S methodologies developed based on RGP, with the corresponding E3S classification of SSCs that deliver the functions.

Codes and standards used in the design of SSC are commensurate with their safety classification, with higher safety classified SSCs designed to appropriate nuclear industry-specific codes and standards, such as American Society of Mechanical Engineers (ASME) codes.

The E3S design principles have been used to develop E3S requirements that guide and inform the design of SSC to achieve their E3S functions and incorporate RGP. Central to this is design simplicity, prioritising inherent E3S protection and elimination of risks in preference to controlling them in accordance with the hierarchy of controls. Passive means of protection are adopted where practicable, with minimal reliance on operator action or the sustained provision of electrical power.

More stringent E3S requirements are allocated for higher safety classified SSCs, covering design aspects including high reliability and single failure tolerance through provision of redundancy, diversity of initiation between safety measures, facilitation of EMIT, and autonomy without reliance on essential services for 72 hours from onsite mobile equipment, or 168 hours from off-site equipment. A summary of the E3S requirements is presented in E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21]. The allocation of E3S requirements to the site, plant, or SSCs is integral to the design process and feeds into the wider systems engineering requirements definition, governed by the ‘Define and Manage Requirements’ process [25].

Safety analysis has also been used to inform the design of SSCs from the outset of the project, including deterministic, probabilistic, hazards, radiation protection, HF, and conventional safety. The safety analysis is iterative with insights informing the ongoing detailed design, meaning each iteration provides increasing confidence that acceptance criteria can be achieved. Further details on how the suite of analysis has informed the design up to DRP4 is provided in Section 24.3.

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 [4] and within the ‘systems engineering’ E3S Case chapters. At DRP4, the evidence focuses on higher safety classified SSCs that are of a higher level of design maturity; however, the integrated

E3S and engineering design approach and evidence to date provides confidence that the design of all SSCs can reduce risks to ALARP.

24.2.4 Defence in Depth

24.2.4.1 Approach and Implementation

The provision of multiple, independent barriers to provide Defence in Depth (DiD) against the progression of fault sequences is a key deterministic safety approach to support reduction of risks to ALARP. In accordance with international RGP, the E3S design principles require that "Defence in depth against initiating events shall be achieved by the provision of a number of consecutive and reasonably practicably independent measures that would have to fail before harmful effects could be caused to people or to the environment".

For RR SMR, safety measures are employed across all five levels of DiD, where practicable, to deliver the FSFs. Safety measures are designed to minimise susceptibility to failures on one level affecting any other level. This is achieved using different equipment, where reasonably practicable, that are independent and diverse from one another, such that common causes of failure across multiple safety measures and DiD levels are minimised. The safety measure design approach applies a combination of both passive and active safety measures to ensure independence and diversity (see Section 24.2.5).

The RR SMR DiD approach also implements at least two independent and diverse safety measures for frequent initiating events (>1E-03 per year) at DiD 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 approach to DiD is also implemented within the supporting C&I and electrical systems that deliver safety functions as part of the safety measure. C&I independence is implemented using a combination of physical separation, electrical isolation, and functional and communication independence. This includes safety class 1 hardwired and software-based systems that each provide an independent and diverse means of delivering protective safety functions at DiD level 3. Electrical system independence across the levels of DiD is implemented through design features, including trip to house load, DGs for power supply during Loss of Offsite Power (LOOP), and alternate battery-backed power supplies during Station Blackout (SBO).

The approach and implementation of DiD is summarised in E3S Case Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [21], which introduces the safety measures at each level of DiD in the reactor, waste systems, and fuel route. Chapter 3 demonstrates that there is substantial DiD within the design to deliver each of the FSFs, with safety measures being designed in accordance with the E3S design principles to ensure independence and diversity, where practicable. Further details of the DiD safety measures for each Postulated Initiating Event (PIE) and operating mode are presented in the Fault Schedule [26].

Whilst substantial levels of DiD are incorporated across the power station, the design of safety measures for the fuel route, including the Spent Fuel Pool (SFP) [FAB10] and the fuel handling systems, is generally of lower maturity than for the reactor systems at DRP4. As such, there is less evidence within Version 3 of the E3S Case that the fuel route safety measures can deliver FSFs to implement the DiD approach. However, the safety functions to be delivered are established and the safety measures (and SSC that comprise them) are identified in the Fault Schedule [26]. The fuel route measures are being designed in the same manner as for reactor systems, incorporating RGP and OPEX in accordance with the E3S design principles, as described Section 24.2.3. Furthermore, iterative analysis is continuing to feed into the design of fuel route safety measures, and the results

of the deterministic analysis evidence presented in E3S Case Tier 1 Chapter 15: Safety Analysis [18] support the conclusions that acceptance criteria can be achieved. Further evidence to underpin claims that fuel route safety measures (and all safety measures) can achieve their FSFs and achieve their acceptance criteria will continue to be presented in future versions of the E3S Case, including expansion of the Probabilistic Safety Assessment (PSA) to evaluate against numerical risk targets.

24.2.4.2 Independence and Diversity of Safety Measures

The implementation of DiD within the design aims to ensure independence and diversity between safety measures across the DiD levels, as described in Section 24.2.4.1. However, this may not always be practicable to achieve. Therefore, SSCs that share equipment between levels include a comprehensive evaluation to ensure risks remain acceptable and can be reduced to ALARP.

For example, the primary safety measures delivering reactor CoFT at DiD level 3 are the safety class 2 Passive Decay Heat Removal (PDHR) [JN02] and the safety class 1 Emergency Core Cooling (ECC) [JN01]. The majority of the SSCs that comprise each of these safety measures are independent and diverse from each other, however, there are several key components that are shared, including the Local Ultimate Heatsink System (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] 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] 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.

It is also recognised that components like the Reactor Pressure Vessel (RPV) [JAA] are shared between all levels of DiD. It is not considered reasonably practicable, or even possible, to provide independence for such components and structures, and they are designed to enhanced levels structural integrity to ensure their reliability.

Further details on the levels of independence and diversity between safety measures and the evaluation of risks are presented in the ALARP Summary Report [4].

24.2.5 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 in Section 24.2.3. 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 DiD.

For the key reactor safety measures providing the FSF of CoFT at DiD levels 3 and 4, the ECC [JN01], PDHR [JN02] and IVR [JM02] 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 defence in depth is provided through active means.

For the key reactor safety measures providing the FSF of CoR at DiD level 3, the Scram [JD01] safety measure provides the primary passive means of shut down and reactivity hold down for the reactor through control rod release under gravity, whilst the diverse ASF [JD02] provides the secondary active means through pumped injection of potassium tetraborate into the core.

For the SFP [FAB10], both active and passive safety measures maintain CoFT for spent fuel storage at DiD level 3. The Faulted Fuel Pool Cooling [FA02] safety measure uses an active cooling chain to transfer heat to the atmosphere via a heat exchanger arrangement to the Component Cooling System (CCS) [KAA] and ESWS [PB]. The Fuel Pool Boil-Off (FPBO) [FA01] provides a passive means to ensure the fuel assemblies remain covered following loss of active cooling.

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.

Further details on the passivity of safety measures are presented in the ALARP Summary Report [4].

24.2.6 Design Features

24.2.6.1 Introduction

The RR SMR is generally based on established PWR 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 [4]. Key design features are summarised below.

24.2.6.2 Chemistry

24.2.6.2.1 Boron-free Chemistry

All extant commercial PWRs 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 reactivity hold down achieved by the control rods alone.

The design decision to adopt a boron-free chemistry regime [27] was undertaken early in the design programme, based on a review of RGP and OPEX, and an evaluation of the advantages and disadvantages against a plant design that uses soluble boron for normal operations reactivity control. There is limited RGP for boron-free PWR designs, however, OPEX is gained from Boiling Water Reactors (BWRs), which demonstrates the use of reactivity control without boron.

Clearly, the use of boron for duty reactivity control is considered RGP for PWRs and is a well understood and developed solution. However, the boron-free approach also adheres to RGP including application of the hierarchy of controls, such as substantial reduction in the generation of tritium such that there is no requirement for tritium discharges to reduce worker doses to acceptable levels (noting that the design is still capable of discharges), and use of passive techniques for safety measures.

There are significant E3S advantages of boron-free chemistry, including:

- It avoids concerns with boric acid induced corrosion of pressure vessels, bolting and other critical components in the event of a RCS [JE] 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, there are potential disadvantages to adopting boron-free chemistry. Borated designs require comparatively fewer control rods and Control Rod Drive Mechanisms (CRDMs), and a higher CRDM packing density presents challenges including geometric clashing, CRDM cooling effectiveness, and Electromagnetic Interference (EMI). The core and CRDMs are being designed to address these challenges, with analysis providing confidence that CRDMs can achieve their safety functions. Further details on the CRDM design and analysis will be provided in E3S Case Tier 1, Chapter 4: Reactor (Fuel and Core) [28]).

A further potential disadvantage is identified during the RPV [JAA] Upper Internals lifting operation for refuelling. In traditional PWRs, the concentration of soluble boron in the primary coolant is raised prior to this lift to provide reactivity suppression in the event of inadvertent control rod withdrawal. Conversely, a boron-free design is reliant on detecting if there is a fault which prevents rods remaining in the core. This challenge is addressed through both engineered measures adopted in the design of the upper internals and operational measures during lifting, described in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [29]. Given the maturity of the fuel route safety measure design at DRP4, further evidence is required to fully verify that safety functions can be delivered during refuelling and appropriate levels of DiD are achieved. This will be presented in future versions of the E3S Case.

Overall, the evaluation of options concludes that both boron and boron-free designs can reduce risks to levels that are acceptable, which supports the boron-free decision for RR SMR. A more detailed evaluation of the advantages and disadvantages of boron vs boron-free reactivity control is presented in the ALARP Summary Report [4].

A materials and chemistry Verification and Validation (V&V) programme is ongoing with the aim to demonstrate that the RR SMR primary coolant chemistry regime is at least ‘no worse’ than a widely adopted PWR primary coolant chemistry regime. The testing programme at DRP4 supports this assumption, noting that further confirmatory evidence will be presented as the V&V programmes continue. Further details are described in E3S Case Tier 1, Chapter 20: Chemistry [30].

24.2.6.2.2 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. Other options were considered, such as Sodium Hydroxide, however, they were discounted as either not credible or inferior to Potassium Hydroxide and Lithium Hydroxide.

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.

The boron-free Potassium Hydroxide chemistry regime adopted by RR SMR requires qualification through the V&V test programmes. At DRP4, outputs from these test programmes provide confidence that the chemistry can be underpinned and predicts that Potassium Hydroxide corrosion performance is at least comparable to Lithium Hydroxide and is most likely to be better. Further details are described in E3S Case Tier 1, Chapter 20: Chemistry [30], noting that further confirmatory evidence will be presented in that chapter as the V&V programmes continue to be undertaken.

24.2.6.3 Seismic Isolation System

One of the key design objectives is to be able to construct the RR SMR in a wide variety of locations. This means that the ground conditions and the site-specific seismic hazard the RR SMR is founded on is likely to be different at each site. However, the RR SMR design intends to be as repeatable as possible between sites. Therefore, one of the innovative technologies for RR SMR is the implementation of the Seismic Isolation System (SIS).

The SIS is supported from the raft foundation and comprises a series of Reinforced Concrete (RC) pedestals and Aseismic Bearings which support the Basemat. The Aseismic Bearings protect SSCs above the Basemat by attenuating lateral seismic loads between the Basemat and the pedestals. 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.

Base isolation has been used extensively in non-nuclear buildings, and RGP and OPEX for the application in nuclear facilities exists for six PWRs located at two sites in France and South Africa. Two ongoing nuclear construction projects also utilise seismic isolation devices. RGP also exists within ONR research [31] and IAEA guidance [32] to support the technical basis for the design of SISs for Nuclear Installations, which draws on practices established by authoritative nuclear bodies. These sources of RGP have been used in the design of the SIS.

The design of the SIS and analysis undertaken to date is summarised in E3S Case Tier 1, Chapter 9B: Civil Engineering Works and Structures [33]. There are no specific nuclear specific codes and standards for seismic isolation, and so a collection of nuclear specific seismic design codes and non-nuclear specific design codes are drawn upon and justified. Structural analysis undertaken up to DRP4 indicates that the SIS can achieve its safety functions, noting that further analysis evidence is required and a type testing programme has been established to support V&V. Further work is also established to verify performance during a fire, and a replacement strategy in coordination with the Aseismic Bearing supplier.

The use of RGP and OPEX from similar applications to inform the design of base isolation is a central part of the ALARP demonstration. Structural analysis undertaken to date to verify the application of seismic isolation to the RR SMR provides confidence that the safety functions can be achieved, which once verified will support reduction of seismic hazard risks to ALARP. Further structural analysis and outputs of testing programmes to enhance confidence in this position will be presented in future versions of the E3S Case.

24.2.6.4 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 [JN01] operation. Further information on the ECC [JN01] and operation of the EBD valve is provided in E3S Case Tier 1, Chapter 6: Engineered Safety Features [34].

Options for passive and active (C&I based) means of achieving automatic depressurisation have been evaluated [4]. A key safety benefit of the passive EBD valve is protection against spurious opening of the depressurisation line in normal operation that results in a LOCA, for which the EBD valve provides functional diversity. The adoption of the passive EBD valve is supported by analysis, as PSA evaluation against numerical targets demonstrates that it supports a substantial reduction in spurious line opening frequency and Core Damage Frequency (CDF) contribution from the fault, whilst maintaining Automatic Depressurisation System (ADS) [JNF] reliability [35].

Therefore, the innovative development of the passive EBD valve supports development of the highly reliable passive safety class 1 safety measure that can reduce risks to ALARP. Safety analysis of the ECC [JN01] at DRP4 presented in E3S Case Tier 1 Chapter 15: Safety Analysis [18] support the conclusions that acceptance criteria can be achieved.

A V&V programme is being implemented for the EBD through a series of inspection, analysis and rig testing programmes, including qualification against the ASME QME-1 code. The outputs of these V&V activities will be reported in future versions of the E3S Case to provide further underpinning evidence that the ECC [JN01] can achieve its safety functions and meet acceptance criteria.

24.2.6.5 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 are being 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, 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, described in the Modular Kit of Parts (MKoP) Strategy [36].

The RR SMR modularisation approach reduces risk during manufacture, assembly, installation, and commissioning. For example, maximising offsite build and assembly, and simplifying interfaces (plug and play) can significantly reduce the potential for errors and reduce construction risks, offering significant conventional safety benefits.

Standardisation of the design and modules also provides potential safety and environmental benefits, such as reducing the number of part types to increase reliability, and simplification of 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 E3S, such as requirements for diversity.

Modules are being designed in accordance with the E3S design principles, with bounding E3S requirements and constraints allocated to inform the design of modules, for example fire withstand or radiation shielding requirements. The E3S design principles and requirements feed into the MKoP, which is a library of standardised components that can be configured and used by the layout design 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, the MKoP, and the relevant E3S requirements which will continue to be allocated through iterative safety analysis.

A key aspect of modularisation to be finalised is the treatment of pipes and cables between modules to ensure E3S requirements are achieved, in particular maintaining reliability of module-to-module joints. At DRP4, it is anticipated that installing pipes and cables in-situ onsite, as opposed to installation in the factory with connection onsite, will meet reliability requirements through minimising the number of cable joints. Further evidence to support a final decision will be presented in future versions of the E3S Case.

The areas of the plant that deploy the MKoP will undergo verification activities to demonstrate that modules (or module clusters) can achieve their E3S requirements (and other requirements). The approach to MKoP V&V follows the same approach adopted by other SSCs. At DRP4, a verification strategy for the MKoP is developed, and evidence from the outputs of these activities will be presented in future versions of the E3S Case to demonstrate that E3S requirements can be achieved in the as-build design.

Overall, the modularisation strategy and MKoP design incorporates E3S requirements and aims to minimise any additional risks over traditional construction methods. The benefits of standardisation are well documented in industry, and the strategy is to ensure diversity for risk reduction is not compromised. At Version 3, there is confidence that the approach can provide safety benefits, in particular during the construction and installation phase. The verification that modules can achieve their E3S requirements will provide key evidence for future versions of the E3S Case to underpin claims on modularisation.

Further details of the modularisation strategy to achieve build certainty are summarised in E3S Case Tier 1, Chapter 14: Plant Construction and Commissioning [37].

24.3 Analysis Informed Design

24.3.1 Deterministic Analysis

24.3.1.1 Design Basis Conditions and DEC-A

Deterministic analysis techniques are used to formally identify and assess design basis faults and Design Extension Conditions (DEC) without significant core damage (DEC-A), to provide requirements for safety measures, and demonstrate their suitability, to reduce radiological doses and risks to levels that are ALARP and to systematically inform and improve the RR SMR design.

The systematic process of hazard identification has been used to review and inform the developing design from the outset 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 [38].

The Fault Schedule [26] collates PIEs that have been identified, sentenced and grouped through the safety analysis process and identifies safety measure defence across all five levels of DiD, for all operating modes. Safety measures allocate safety categorised functional requirements onto the design of SSCs that comprise them, including support systems such as C&I, emergency power supplies and the Heating, Ventilation and Air Conditioning (HVAC) systems.

Appropriate deterministic performance analysis methods are used to assess the fault sequences, informed by the Fault Schedule [26], to provide high confidence that safety measures can achieve their safety functions and meet relevant acceptance criteria with suitable margin.

The analysis undertaken up to DRP4 is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [18]. The analysis is iterative by nature and therefore has been undertaken on maturity points that precede the DRP4 design. The design delta is assessed to ensure suitability for underpinning the analysis conclusions of the DRP4 design. Analysis is presented for bounding faults, with arguments for why these faults are bounding. The results and assessment of each fault include a comparison against relevant acceptance criteria and a judgement on the risk position at DRP4.

For each fault sequence analysed, it is shown that acceptance criteria can be met and judged that risks can be reduced to ALARP. This reflects the good practice of performance analysis being used to inform the design of safety measures and SSCs from the outset of the project (as described in Section 24.2.3), which drives design optimisation towards achieving the safety functions and reducing risks to ALARP.

At DRP4, bounding arguments are made where possible, however the full scope of faults requires further analysis evidence. Whilst this presents a risk in the verification of SSCs achieving their safety functions, confidence that acceptance criteria can be achieved is gained through the ongoing analysis and design optimisation process described in Section 24.2.3. Further focus areas are identified, including analysis of shutdown, reactivity and fuel handling faults to determine performance against acceptance criteria, and further exploration of faults to identify additional risk reduction measures, including LOCAs outside containment and Steam Generator Tube Rupture (SGTR). The outputs of further analysis will be presented in future versions of the E3S and will provide key evidence to increase the levels of confidence that risks can be reduced to ALARP.

24.3.1.2 Severe Accident Analysis (DEC-B)

Low frequency events that are more severe than considered within design basis include DECs with significant core damage (DEC-B). Severe Accidents Analysis (SAA) techniques support the

demonstration of 'practical elimination' of large or early releases of radioactive material to the environment through the RR SMR design, and safety measures can either prevent or mitigate associated severe accident phenomena to protect the integrity of the final confinement barrier.

The approach to SAA and practical elimination of severe accident phenomena is presented in E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21], which includes an overview of the functions delivered by the Severe Accident Containment [JM02] safety measure which supports mitigation of severe accidents. The demonstration that severe accident phenomena that can result in a large or early release are practically eliminated (or risks reduced to ALARP) is presented in E3S Case Tier 1 Chapter 15: Safety Analysis [18].

Measures are identified for each limiting DEC-B scenario and analysis for each concludes that acceptance criteria can be achieved and a severe accident safe state can be reached, highlighting areas of uncertainty in the model that are to be addressed through progressive analysis. For phenomena (and event sequences) that could result in a large or early release, where Level 2 PSA results are available, it is demonstrated that the practical elimination target (the occurrence of severe accident phenomena and individual sequences that can result in a large or early release is less than 1E-7/yr [21]) is met with sufficient margin to the targets that provides confidence that risks can be reduced to ALARP as the PSA and SAA progresses.

As the SAA is developed, it will continue to inform the Severe Accident Containment [JM02] safety measure design as part of the design process (as described in Section 24.2.3) to drive design optimisation towards achieving the safety functions and reducing risks to ALARP.

24.3.2 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 [21] to demonstrate that risks are acceptable and can be reduced to ALARP. The PSA is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [18].

PSA has been employed from the early stages of the RR SMR design programme up to DRP4, 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. Due to the iterative nature the analysis and design, the inputs to the PSA generally represent DRP2, which have informed the design and feeds into DRP4. Whilst there is a natural lag between the design and the PSA, insights from the PSA have been used to inform developments and improvements to the design at DRP4 and will continue throughout the remainder of the detailed design phase, to provide confidence that risks are being progressively assessed and reduced such that the design can ultimately achieve numerical risk targets.

At DRP4, the scope covers Level 1 and Level 2 PSA, noting there are exclusions from the scope at this stage which will be incorporated into further iterations. The Level 1 PSA covers operating modes 1 to 6A (excluding 6B) and only reactor fault. The Level 2 PSA covers operating modes 1 and 2 and only the reactor building is modelled. An assessment of all limitations of scope on the RR SMR PSA risk insights are considered, with limitations classified, qualified and where possible quantified to provide an estimate of how the resolution of each limitation could be expected to impact the PSA numerical results.

The Level 1 PSA calculates a CDF of {REDACTED} per year of power operation, which is lower than the previous analysis at DRP1 and is working towards the RR SMR design target of 1E-07 per year. The PSA results provide insight and confidence that the RR SMR presents a balanced design; ICFs collectively account for 32 % of plant fault CDF, with loss of electrics faults accounting for 16.9 %, and LOCA faults accounting for 51.1 %.

The Level 2 PSA calculates a Large or Early Release Frequency (LorERF) of {REDACTED} per year of operation. This is approximately {REDACTED} smaller than the RR SMR LorERF design limit of 1E-06 per year, and {REDACTED} larger than the design target of 1E-08 per year. This is the first output from Level 2 PSA and the baseline value provides confidence that design limits will be met, and design targets are being worked towards. The scope of the Level 2 will continue to be expanded in the next version of the E3S Case and further insights will be gained on the level of risk reduction as the detailed design progresses.

The use of PSA to inform the design from an early stage and the outputs of the PSA undertaken up to DRP4 provide confidence that risks are being reduced, and can be reduced, to ALARP. The limitations of the PSA model at DRP4 are understood and documented. Insights from the PSA and assessment of limitations have informed further work to refine the model and target areas of increased risk. This includes key contributors such as Common Cause Failures (CCFs) and operator actions, which are being used to identify improvements to diversity and definition of operator procedures.

24.3.3 Internal Hazards Analysis

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

The RR SMR is being designed to E3S design principles that inherently drive the layout and SSCs to prevent and protect against hazards, primarily through inclusion of redundancy within headline safety systems that perform their safety functions at DiD Level 3, and segregation of those trains such that a hazard may cause damage to one of those trains only. Methodologies for IH identification and analysis have been developed based on RGP and implemented, including identification of IHs through iterative layout and design reviews, screening of individual and combinations of IHs, and analysis of IHs to specify hazard loadings and allocate IH requirements to protection measures to inform their design optimisation, where necessary.

The IH methods, approaches and overview of protection measures is presented E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21], where protection measures are identified for all identified IHs. Outputs of the IH analysis are presented in E3S Case Tier 1 Chapter 15: Safety Analysis [18]. At DRP4, the majority of IH confirmatory analysis is based on DRP2, with a focus on operating mode 1, which has informed the design up to DRP4. However, design for IH resilience in accordance with the E3S design principles is undertaken for all modes and plant locations, such that there is confidence that claims on IH tolerance can be underpinned through the analysis. Work to assess changes from DRP2 to DRP4 is ongoing and will be reported in Version 4 of the E3S Case. The analysis is generally undertaken on a conservative basis to de-risk the design and provide confidence that the identified protection measures will be capable of withstanding the final hazard loadings from the detailed hazard analysis.

An enhancement for Version 3 of the E3S Case is the development of a Hazards Schedule and Indicative Loads Schedule, which tabulate the outputs of the IH analysis and provide key interfaces to the engineered protection measures being claimed by IHs. These schedules provide clarity on the IH analysis outputs and are being used to identify areas of further work, including areas where unnecessary conservatisms can be minimised, and impacts of design changes that required further assessment. The Hazards Schedule provides a key tool to support the golden thread and guide the work required to support the V&V and guide the necessary evidence to underpin IH claims through detailed design.

The fundamental IH protection measures are incorporated into the design at DRP4, noting the iterative nature of the IH analysis will likely result in further design optimisation as the detailed design progresses. For example, design requirements for segregation and withstand of cable routes for tolerance to IHs are adopted, however, further IH analysis on specific cable routes may require some further design optimisation. Design changes since DRP2 are reviewed and areas of focus for further analysis on DRP4 are presented in E3S Case Tier 1, Chapter 15: Safety Analysis [18], which provides confidence that key risks are understood and will be addressed. It is noted that the methods for V&V of IHs are established at DRP4, however the verification of IH measures is not presented at Version 3. This will be an area of focus in future versions of the E3S Case to provide further evidence that risks can be reduced to ALARP.

24.3.4 External Hazards Analysis

EH 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 EHs.

The Generic Site Envelope (GSE) for the RR SMR is summarised in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [39]. EH applicable to the generic site are identified, screened and characterised, with hazard frequency and severity parameters determined that are relevant to Great Britain (GB). Due to the nature of some EHs being site dependent, the GSE has been developed on a conservative basis to encompass a wide range of potential sites.

The scope of the EH analysis incorporates RGP and assesses both EHs and combinations of EHs. The effects of climate change over a 100-year period following initial deployment are incorporated into parameters, covering the design operational life of the RR SMR, potential lifetime extension and estimated decommissioning period. This supports claims made on the design to deliver fundamental functions through-life.

EH challenges are derived from the list of applicable EHs, grouped according to the engineering challenges that are to be addressed/protected. The EH challenges and overview of protection measures is presented E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21], where protection measures are identified for all identified EHs. Key design features that provide protection measures against EHs include the:

- Hazard Shield, a reinforced concrete structure providing aircraft impact protection to SSCs (and protection against other EHs) which are required to deliver and maintain the plant in a stable, safe state.
- SIS, as described in Section 24.2.6.3.

The plant layout has been systematically optimised during the design development to reduce risks from EHs (including combined hazards). Layout requirements for SSCs supporting a safety category A or B function or a severe accident mitigation measure are, where practicable:

- Positioned inside the Hazard Shield, thus achieving enhanced resilience to (tornadic) storm, flooding/ water ingress, etc. EH challenges.
- Positioned on the SIS, thus achieving enhanced resilience to seismic events and reducing the burden of seismic qualification.
- In the case of systems external to the Hazard Shield, designed with redundancy, maximised separation and location consideration, thus achieving increased functional resilience against accidental aircraft crashes and wind induced debris impacts. For example, the two redundant DGs that supply power supply during LOOP are segregated to the north and south of the site.

This provides confidence at Version 3 of the E3S Case that risks can be reduced to ALARP, noting that detailed analysis and V&V is still required. The analysis methods for EHs are summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [18]. These cover key areas of focus for EHs, such as aircraft impact assessment and space weather hazards. The consideration of the space weather EH is a relatively new concept in safety cases and represents good practice to ensure appropriate protection can be provided in the design. A methodology is also developed to consider beyond design basis EHs and address potential cliff-edges, representing RGP.

Evidence of the application of the EH methodologies, and the V&V of SSCs that deliver the protection measures against EH challenges, is not presented at Version 3 of the E3S Case. The principles of redundancy and separation/segregation, and the design of SSCs to the bounding and conservative parameters and loadings in the GSE, provides a degree of confidence that protection measures will be able to address the EH challenges posed. Structural analysis of the Hazard Shield and SIS also provides confidence that safety functions and tolerance to EHs can be achieved. The outputs of the application of EH methodologies and V&V of the EH protection measures will therefore be an area of focus in future versions of the E3S Case to provide further evidence that risks can be reduced to ALARP.

24.3.5 Radiation Protection

The E3S design principles relating to radiation protection are expanded upon through radiation protection policies for dose management, source term, and radiation shielding, which together aim to ensure that radiation exposure of employees and other persons is kept to levels that are below legal limits and are ALARP. Practical guidance on the application of the principles outlined in the policies is provided through radiation protection guidelines, which are used to influence the design during optioneering, and used to derived radiation protection requirements that are allocated to the layout and design of SSCs.

There are key areas where radiation protection principles have influenced design at DRP4. These are summarised in the radiation protection ALARP topic report [40], which concludes that 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 to workers and the public is summarised in E3S Case Tier 1, Chapter 12: Radiation Protection [17]. The assessment demonstrates that radiation worker doses can be reduced to 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.

Much of the assessment presented is based on a previous DRP to inform DRP4, and whole suite of updated assessments is planned for the DRP4 design that will be presented in Version 4 of the E3S Case. This means that outputs of dose assessments do not reflect the most current design, and further optimisation is likely. However, the principles of radiation protection are being used to drive dose rates to ALARP through spacing in the layout and through shielding provisions, and examples are provided for how the assessment has informed the shielding thicknesses in the DRP4 design.

At DRP4, the focus of the generic design is to ensure the principles of dose rate reduction continue to be applied to the layout and SSC design. Progressive assessments have been undertaken and evaluated against numerical targets to inform design optimisation. There is confidence that the design is being sufficiently optimised for radiation protection such that a robust ALARP demonstration can be developed in future iterations of the case. A key area of focus for the progressive analysis is to develop more specific operating procedures and EMIT tasks, to build

further confidence in the worker dose assessments, which are currently based on OPEX data for high dose tasks.

24.3.6 Human Factors Analysis

HF have been integrated within the RR SMR programme since its early conception, through a programme of iterative HF activities set out in the Human Factors Integration Plan (HFIP). These activities include systematic identification of human errors and design mitigation, minimising Allocation of Functions (AoFs) to manual tasks, task analysis to verify AoFs, and implementation of a Human Machine Interface (HMI) style guide to the design of SSCs and the control rooms, The activities are summarised in E3S Case Tier 1, Chapter 18: Human Factors Engineering [19].

RGP for HF is therefore incorporated within the RR SMR design at DRP4. As the design develops, AoF will continue, supporting an optimised combination of human and engineered elements of the whole power plant design whilst meeting the design principle for systems to be passive or automated where possible, which supports reduction of risks to ALARP.

The RR SMR approach guided by the E3S design principles is to reduce reliance on operator actions, particularly for safety category A and B functions, which limits the claims made on the operator through the safety analysis. However, there are operator actions derived from the Fault Schedule and the PSA, required to perform a number of normal operational duties during power and shutdown operations, monitor the initiation of safety systems, and contribute to the longer-term management of safety systems and emergency arrangements. At DRP4, a small number of operator actions are identified, which are substantiated, and similar methods will be used to provide confidence that further operator actions identified can be substantiated.

24.3.7 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 Integrated Management System (IMS) processes, rather than undertaken as auxiliary activities, as can often be the practice.

Rolls-Royce SMR Limited undertakes the principal designer and designer roles during the generic design stage, including the duties of providing plans, and undertaking monitoring and co-ordination of health and safety communication across all disciplines during the pre-construction stage. This primarily covers ensuring that those involved have the skills, knowledge and experience, or organisation capability to fulfil the required health and safety roles. Another key requirement is the undertaking of appropriate risk assessments and the incorporation of risk minimisation measures during all lifecycles.

Meeting legislative requirements, including those for conventional safety, is part of the E3S criteria that are evaluated against as part of the design optioneering and recorded as part of the design decision records, described in Section 24.1.2. Furthermore, conventional safety and fire requirements are established and informing the layout development, as described in E3S Case Tier 1 Chapter 3: E3S Objectives and Design Rules for SSCs [21]. These have informed the inherent features to eliminate risks, such as minimising confined spaces, and also risk mitigation measures, such as fire barriers and escape routes, which provides confidence that SSCs and the layout are being designed to minimise conventional safety risks. Details of the design optimisation for the

conventional safety is summarised in E3S Case Chapter Tier 1, Chapter 22: Conventional & Fire Safety [20].

The IMS conventional safety processes mandate that risk assessments are undertaken throughout the design development process, including:

- Design Risk Assessments (DRAs) to support hazard identification during the design of components/equipment and modules/clusters.
- Lifecycle Risks Assessments (LRAs) to support hazard identification during the design of layout, operations, maintenance, construction, manufacture, commissioning and decommissioning.
- Hazard identification studies, such as Hazard & Operability (HAZOP).

At DRP4, conventional health and safety design guidance supports design optioneering in accordance with IMS processes [13]. The production of DRAs and LRAs continues to be developed and is identified as a focus area for conventional hazards, with further risk assessments (and other conventional safety risk reduction activities) expected to be implemented to provide evidence for Version 4 of the E3S Case.

24.4 Risk Reduction Through-Life

24.4.1 Construction

At DRP4, the construction approaches are being developed in accordance with applicable legislation, including the Construction (Design and Management) Regulations 2015, and other sources of RGP and OPEX related to construction of nuclear power plants. The construction approaches are driven by the build certainty objectives for the RR SMR, including maximising the use of modularisation and adopting a site factory for construction and installation. The approaches will employ Modern Methods of Construction (MMC), which aim to deliver and improve significant levels of safety compared to traditional construction methods to reduce nuclear and conventional health and safety risks to ALARP.

Maximising the use of modularisation can reduce on-site complexity, such that on-site activities are focused where possible on lifting and placement, jointing and final commissioning. For example, the Civil Kit of Parts (CKoP) approach enables construction of certain civil components (e.g., cellular retaining walls) either off-site or on-site prior to lifting into their intended location, with in-situ concrete pours where necessary, to reduce the number and frequency of lifts and associated lift-related hazards. Furthermore, the MKoP approach can offer safety benefits to reduce risks to ALARP, described in Section 24.2.6.5 of this chapter.

The 'Site as a Factory' approach provides an environmental shelter for Reactor Island construction activities, with a controlled environment for up to 24 hours a day, 365 days a year. This is a different approach to traditional nuclear power station construction, primarily to ensure productivity and build certainty. It can also offer conventional health and safety benefits, for example, optimising deliveries and lifting of materials to reduce manual handling. Such benefits are being considered as the approach is developed and implemented.

Further details on the construction approaches are summarised in E3S Case Tier 1, Chapter 14: Plant Construction and Commissioning [37].

24.4.2 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 of the commissioning strategy are summarised in E3S Case Tier 1, Chapter 14: Plant Construction and Commissioning [37].

24.4.3 Operations

The design is being developed for future operation, with a key E3S design objective to minimise reliance on operators (maximising passivity), where practicable, and using RGP to inform the design

of SSCs and the layout with sufficient space to accommodate expected EMIT activities. Design reviews are undertaken by Constellation Energy Corporation, who operate the largest fleet of nuclear plants in the United States, which feed into the design development process.

Operating philosophies are developed alongside design, and processes are being developed to transfer OLCs from the design and E3S analysis into operational documentation, such as Technical Specifications and Severe Accident Management Guidelines (SAMGs). This provides confidence that the RR SMR will be operated in line with the design intent and the requirements of the E3S Case and reduce risks to ALARP.

Further information on the operational aspects of the RR SMR is summarised in E3S Case Tier 1, Chapter 13: Conduct of Operations [41] and E3S Case Tier 1, Chapter 16: Operational Limits and Conditions for Safe Operation [42].

24.4.4 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 support decommissioning and minimisation of waste [4], including features such as decay storage of resins/concentrates to reduce Intermediate Level Waste (ILW) volumes, and use of back-washable filters that do not require filter changes and reduce operator maintenance dose.

The RR SMR modularisation and build certainty approach also offers opportunities to reduce risks during decommissioning, including:

- 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 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 on decommissioning strategies is provided in E3S Case Tier 1, Chapter 21: Decommissioning and End of Life Aspects [43].

24.5 Conclusions

24.5.1 Conclusions and Forward Look

This chapter summarises the holistic arguments and evidence for how the RR SMR design reduces risks and exposures to ALARP to achieve the claims in Section 24.0.3. It describes how the ALARP methodology has been embedded within the E3S and engineering processes from the outset of the project, ensuring the design incorporates RGP, uses design optioneering to evaluate safety risks and inform decisions, and assesses risks through iterative safety analysis. This has provided the benefit of continuous and systematic risk reduction as the design matures, as opposed to 'retrofitting' ALARP improvements later in the design stage.

The fundamental selection of proven and well-established PWR technology for the RR SMR, which offers a vast amount of RGP and OPEX to deliver safety. Novel design features such as boron-free chemistry and a SIS are adopted that can provide safety benefits and reduce risks, noting an extensive verification and testing programme is underway to underpin their use. Evidence at DRP4 provides confidence that these design features can be underpinned, however further substantiation is required to increase confidence and demonstrate risks can be reduced to ALARP.

Modularisation is a key innovation in comparison to large-scale nuclear plants. In addition to being a key enabler for build certainty, the modularisation and standardisation approach has potential advantages to reduce nuclear and conventional safety risks through the plant lifecycle. Potential disadvantages are acknowledged, such as reduction in diversity through standardisation, however this is mitigated through the MKoP strategy that incorporates the E3S design principles and bounding E3S requirements into the design of modules, to ensure E3S functions are not compromised.

The layout is being developed to E3S requirements and constraints developed from RGP to drive high levels of inherent safety and eliminate risks where practicable. Whilst the RR SMR has a smaller footprint than large-scale nuclear plants, safety levels are not compromised, with greater emphasis on barrier segregation where spatial separation is not possible. This supports the conclusion that the layout is capable of reducing risks to ALARP. The E3S requirements and constraints allocated to the layout will continue to be refined as safety analysis, in particular IH and shielding/dose rate assessments, iterates with the design. Evidence from these activities is expected to provide further confidence in this ALARP position.

The design incorporates substantial DiD, with multiple layers of safety through provision of safety measures across all five levels. Enhanced DiD is provided in line with UK RGP for DiD level 3, with the provision of two independent and diverse measures for protection against frequent faults. Independence and diversity are incorporated between levels of DiD, or where equipment is shared, ALARP justifications are made. Substantial levels of DiD is extended to the electrical and C&I systems that support delivery of the safety measures, including provision of measures to ensure tolerance to LOOP and SBO.

The SSC design process incorporates extensive optioneering to incorporate RGP and OPEX where available, and down-selection of design options is informed by E3S analysis and evaluation against E3S criteria. SSC are design to deliver E3S functions allocated through analysis, and in accordance with the E3S design principles, including (but not limited to) design simplicity, passivity with minimal reliance on operator actions, and high levels of redundancy to achieve functions.

Safety analysis is a key part of integrated E3S and engineering design processes, and includes deterministic, probabilistic, hazards, severe accident, radiation protection, HF, and conventional and

fire analyses. Analysis is iterative and has been used from the outset of the project to inform optimisation of the design and drive risks below numerical targets to ALARP. Overall, the suite of analysis presented at DRP4 supports the demonstration that risks and exposures can be reduced to ALARP. Focus areas to increase confidence in this position are identified across the suite of analysis, including deterministic assessment of consequences against acceptance criteria, enhancing the scope of PSA models and reducing conservatisms, application of EH methodologies, development of inputs to dose assessments, and increasing conventional risk assessments.

At DRP4, there is confidence that the generic design is being developed and sufficiently optimised to reduce E3S risks, such that a robust ALARP demonstration can be progressively developed in future iterations of the E3S Case.

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

None identified for this chapter at this revision.

24.6 References

[1] Rolls-Royce SMR Limited, SMR0001603 Issue 2, “Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles,” July 2024.

[2] Rolls-Royce SMR Limited, SMR0004294 Issue 4, “Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 1: Introduction,” August 2025.

[3] Rolls-Royce SMR Limited, SMR0002155 Issue 4, E3S Case Route Map, August 2025.

[4] Rolls-Royce SMR Limited, SMR0009086 Issue 3, “ALARP Summary Report,” May 2025.

[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, “C3.2.2-2 Conduct Design Optioneering”.

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

[15] 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].

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

[17] Rolls-Royce SMR Limited, SMR0004139 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 12: Radiation Protection,” August 2025.

[18] Rolls-Royce SMR Limited, SMR0003977 Issue 4, “Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 15: Safety Analysis,” August 2025.

[19] Rolls-Royce SMR Limited, SMR0004520 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, TIer 1, Chapter 18: Human Factors Engineering,” August 2025.

[20] Rolls-Royce SMR Limited, SMR0004367 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 22: Conventional & Fire Safety,” August 2025.

[21] Rolls-Royce SMR Limited, SMR0004589 Issue 4, “Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 3: E3S Objectives and Design Rules,” August 2025.

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

[23] Rolls-Royce SMR Limited, SMR0010121 Issue 2, “CIV-026-Fuelling Block Pool & Pit Configuration Decision Record,” July 2025.

[24] Rolls-Royce SMR Limited, SMR0021396 Revision 1, "RD9 & DR3 Readiness Review – Reactor Island Integration," March 2025.

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

[26] Rolls-Royce SMR Limited, SMR0004444 Issue 4, "Rolls-Royce SMR Fault Schedule (Version 8)," February 2025.

[27] Rolls-Royce SMR Limited, EDNS01000937657 Issue 1, "PCD2 Boron-Free Decision," February 2022.

[28] Rolls-Royce SMR Limited, SMR0004210 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 4: Reactor (Fuel and Core)," August 2025.

[29] Rolls-Royce SMR Limited, SMR0003863 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 9A: Auxiliary Systems," August 2025.

[30] Rolls-Royce SMR Limited, SMR0004982 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 20: Chemistry," August 2025.

[31] ARUP Report on behalf of the ONR,, "ONR895, 292732-02-ONR895-REP001, Independent Research into the Seismic Isolation of SMRs and AMRs," September 2023.

[32] IAEA, IAEA-TECDOC-1905, "Seismic Isolation Systems for Nuclear Installations," 2020.

[33] Rolls-Royce SMR Limited, SMR0003778 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 9B: Civil Engineering Works and Structures," August 2025.

[34] Rolls-Royce SMR Limited, SMR0003771 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 6: Engineered Safety Features," August 2025.

[35] Rolls-Royce SMR Limited, EDNS01000537027/001, "SMR Probabilistic Safety Assessment," March 2021.

[36] Rolls-Royce SMR Limited, SMR0008962 Issue 3, "Modular Kit of Parts Strategy," May 2025.

[37] Rolls-Royce SMR Limited. SMR0004289 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 14: Plant Construction and Commissioning," August 2025.

[38] Rolls-Royce SMR Limited, SMR0006906 Issue 3, Hazard Log Spreadsheet - Version 8, March 2025.

[39] Rolls-Royce SMR Limited, SMR0004542 Issue 4, "Environment,Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 2: Generic Site Characteristics," August 2025.

[40] Rolls-Royce SMR Limited, SMR0007303 Issue 1, "Radiation Protection ALARP Topic Report," January 2024.

[41] Rolls-Royce SMR Limited, SMR0004247 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 13: Conduct of Operations," August 2025.

[42] Rolls-Royce SMR Limited, SMR0004555 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 16: Operational Limits and Conditions for Safe Operation," August 2025.

[43] Rolls-Royce SMR Limited, SMR0004599 Issue 4, "Environment, Safety, Security, and Safeguards Case Tier 1, Chapter 21: Decommissioning and End of Life Aspects," August 2025.

24.7 Abbreviations

ADS	Automatic Depressurisation System
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
ASF	Alternative Shutdown Function
ASME	American Society of Mechanical Engineers
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
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
ECC	Emergency Core Cooling
EMI	Electromagnetic Interference

EMIT	Examination, Maintenance, Inspection and Testing
FAT	Factory Acceptance Testing
FSF	Fundamental Safety Function
GB	Great Britain
GDA	Generic Design Assessment
HAZOP	Hazard & Operability
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
IMS	Integrated Management System
IVR	In-Vessel Retention
LOCA	Loss of Coolant Accident
LoERF	Large or Early Release Frequency
LOOP	Loss of Off-site Power
LUHS	Local Ultimate Heatsink System
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
RC	Reinforce Concrete
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
SAMGs	Severe Accident Management Guidelines
SFAIRP	So Far As Is Reasonably Practicable
SG	Steam Generator
SIS	Seismic Isolation System
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