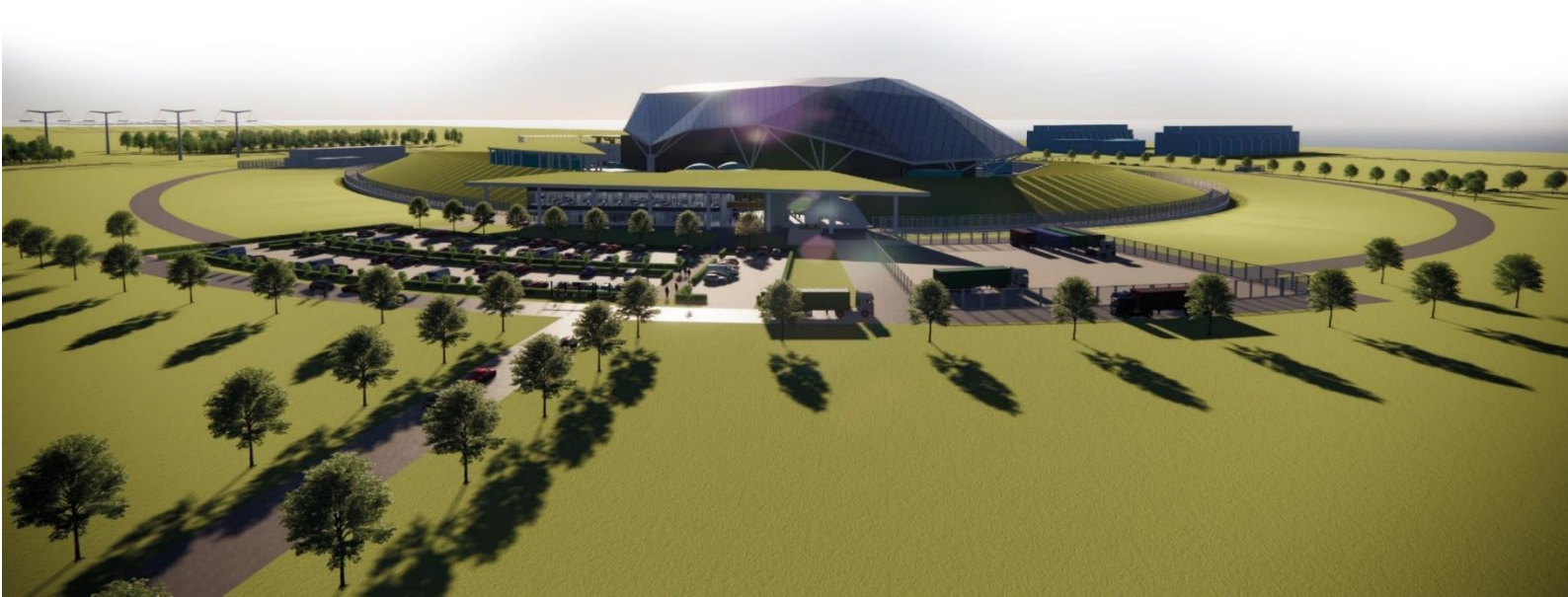
Environment, Safety, Security and Safeguards Case Version 3, Tier 1,
Chapter 3: E3S Objectives and Design Rules for SSCs



Record of Change

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First issue of E3S Case
January 2024	2	Issue	Incorporates revised approaches defined at Reference Design 7, aligned to Design Reference Point 1, including: • Additional information included on safety analysis approaches for severe accidents, probabilistic safety assessment and internal hazards • Summary of Examination, Maintenance, Inspection and Testing approach incorporated • Summary of Verification and Validation approach incorporated Expanded E3S categorisation and classification methodology to include all E3S disciplines
May 2024	3	Issue	Updated to correct revision history status at Issue 2. Chapter changes include: • Clarification of type of Verification and Validation strategies (Section 3.1.7) • Additional detail within Conclusions Section for how arguments and evidence presented meet the generic E3S case objective • Population of the SSC classification table in Appendix B 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 (Section 3.0.3) • Security and environment functions added (Section 3.1.3) • Design approach for radiation protection added (Section 3.1.3) • List of Postulated Initiating Events relevant to RR SMR design and analysis added (Sections 3.1.4 and 3.14) • Application of Defence in Depth approach added, introducing measures to deliver fundamental safety functions (Section 3.1.6) • General design requirements from E3S design principles expanded to plant and layout, and more detail added on approaches for application of design requirements (Section 3.1.7) • Approach to practical elimination of severe accident phenomena added (Section 3.1.8)

Date	Revision Number	Status	Reason for Change
			• Analysis approaches revised to reflect updates to arrangements (Section 3.1.9) • Design approach to ageing management added (Section 3.1.12) • Updated list of E3S classifications (Section 3.15) • Approach to external hazards analysis and design measures added (Section 3.3) • Approach to internal hazards analysis and design measures added (Section 3.4) • Design approach to verification, equipment and seismic qualification added (Section 3.9) • Design approach to Examination, Maintenance, Inspection and Testing added (Section 3.10) • Approach to compliance with E3S design principles added (Section 3.11)

Executive Summary

Chapter 3 of the generic Environment, Safety, Security, and Safeguards (E3S) Case presents the E3S objectives and design rules for the Structures, Systems, and Components (SSCs) of the Rolls-Royce Small Modular Reactor (RR SMR). Version 3 of the generic E3S Case supports and incorporates Design Reference Point 4 (DRP4).

The chapter outlines the arguments and evidence for how the E3S design principles are applied to the design approaches and analysis of the RR SMR, which support the underpinning of the top-level claim that 'Rolls-Royce SMR is designed and evaluated to achieve the E3S fundamental objective to protect people and the environment from harm'. Fundamentally, the E3S design principles are derived and justified based on an extensive set of United Kingdom (UK) and international Relevant Good Practice (RGP).

The fundamental environment, safety and security functions are established, and measures are assigned to deliver them. E3S categorisation and classification methods were developed using RGP. The safety categorisation and classification method is applied extensively to the design of SSCs, to ensure commensurate design codes and standards are applied. SSCs that deliver environmental measures are classified as Key Environmental Protection Equipment (KEPE). Security functions are delivered by the Physical Protection System (PPS) and Cyber Protection System (CPS) which allocate requirements to security classified SSC. Design for safeguards at DRP4 enables the delivery of safeguards functions to SSCs.

Postulated Initiating Events (PIEs) are systematically identified using suitable methods and techniques, which are used to inform the design and safety analysis. Numerical targets for the analysis of the design are based on RGP. The plant states and approach to Defence in Depth (DiD) is presented, which is extensively applied through provision of safety measures that deliver the Fundamental Safety Functions (FSFs) across all DiD levels.

The design approaches and associated E3S requirements are established for the plant, layout and measures, covering both nuclear and conventional safety. Codes and standards are established follow good industry practices, with more stringent requirements for high safety classified SSCs.

The design approaches for ageing management and Examination, Maintenance, Inspection and Testing (EMIT) are developed using RGP. The approach to Verification and Validation (V&V) of the design and SSCs delivering E3S functions is presented, which incorporates Equipment Qualification (EQ). The application of these approaches to the design are presented across the systems engineering chapters of the case.

An extensive summary of the design approaches to internal and external hazards analysis are described, with a comprehensive sentencing of hazards that have informed the levels of hazard protection within the design to maintain delivery of FSFs.

At this stage, the chapter achieves the generic E3S Case objective at Version 3 'to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it's developed through detailed design'. The iterative nature of the analysis means further refinement of functions and measures in future revisions of the E3S Case are likely to support the demonstration of As Low As Reasonably Practicable (ALARP) Best Available Techniques (BAT), and secure/safeguards by design.

Contents

Tables

Figures

3.0 Introduction to Chapter

3.0.1 Introduction

Chapter 3 of the Rolls-Royce Small Modular Reactor (RR SMR) generic Environment, Safety, Security and Safeguards (E3S) Case presents the general principles, concepts, requirements, codes and standards for the design and evaluation of the RR SMR to achieve its E3S objectives. It sets out the general E3S design basis that drive the design of the plant and Structures, Systems and Components (SSCs), with reference to other chapters of the E3S Case that demonstrate compliance.

3.0.2 Scope and Maturity

The scope of this chapter covers how the E3S design principles [1] are applied to the design and analysis of the RR SMR. The E3S design principles provide the framework for generic design and verification of SSCs important to E3S, and the plant layout, to ensure the E3S fundamental objective can be met at all lifecycle stages. Compliance with the principles is demonstrated across other chapters of the case; this demonstration is presented through arguments and evidence to underpin claims that are aligned to the principles (see Section 3.0.3).

The chapter covers the analysis approaches to derive and allocate E3S functions to measures to achieve the fundamental functions. The analysis topics within scope include deterministic, severe accidents, Internal Hazards (IHs) and External Hazards (EHs), Probabilistic Safety Assessment (PSA), environmental, security and safeguards. The design approaches for radiation protection, human factors, and conventional health and safety are covered in this chapter, with reference to respective E3S Case chapters for detailed analysis methods.

The measures assigned to achieve E3S functions across the levels of Defence in Depth (DiD) are introduced within this chapter, including those providing internal and external hazard protection. The applicable requirements derived from the E3S design principles that apply to the design of those measures are also specified. Further detail on the design of measures and SSCs to achieve their functions is presented in the Tier 1 systems engineering chapters of the case.

The scope covers the categorisation and classification method and its application to SSCs that deliver E3S functions. This includes safety, environmental, security and safeguards classification, in addition to seismic performance classification. Classifications of all SSCs within the scope of the generic E3S Case are listed.

The chapter also covers the general design approaches to Examination, Maintenance, Inspection and Testing (EMIT), ageing management, and Equipment Qualification (EQ) through verification. The outputs of the application of these approaches to SSCs are covered within the relevant systems engineering chapters of the case.

The scope of this chapter does not include the detailed analysis methods by which the design aspects are evaluated, such as (but not limited to): methods for compliance with structural integrity defect tolerance assessments, shielding assessment methodology for radiation protection, human factors analysis, or analysis methodology for assessment of IHs and EHs. These methods and the outputs of their application through confirmatory analysis are described within the associated analysis chapters of the case.

The principles for design and operation of site factories, site-specific aspects (largely multi-unit effects) and land quality management are not set by the generic design and are all out of scope.

Version 3 of the generic E3S Case supports and incorporates Design Reference Point 4 (DRP4). At DRP4, the E3S design principles are well established based on Relevant Good Practice (RGP) to set the framework for the design and analysis. As such, no significant changes to the E3S design principles are expected in future revisions of the generic E3S Case.

Safety functions are identified through development of the Fault Schedule, which at DRP4 is matured for all modes of operation for design basis faults, IHs and EHs, non-fuel melt accidents, and severe accident core-melt scenarios. Whilst no fundamental changes are expected for the generic E3S Case, increased detail will be reflected in future revisions as the Fault Schedule naturally iterates with the detailed design and supporting analysis.

Fundamental Environment Functions are established for the design. Environment measures that deliver them are listed, which support the claims for demonstration of Best Available Techniques (BAT). Measures will continue to be reviewed and identified as the environmental assessments iterate through detailed design and the site-specific cases.

Physical and cyber security functions are identified for the security systems. The case also identifies any engineering or layout SSCs that contribute to the delivery of the security functions.

Safeguards functions are not yet allocated to SSC, however, non-functional requirements are established and allocated to the layout and relevant fuel route SSCs to facilitate the provision of safeguarding equipment in the detailed design.

The method for E3S categorisation and classification, including seismic performance classification, is established based on RGP for each E3S discipline. At DRP4, measures and associated SSCs that are allocated an E3S function are assigned E3S and seismic performance classifications.

3.0.3 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 3 is developed from the top-level claim that ‘the Rolls-Royce SMR is designed and evaluated to achieve the E3S fundamental objective to protect people and the environment from harm’.

Chapter 3 primarily presents information to underpin the first level sub-claim [Sub-Claim 3.1] ‘the fundamental functions are achieved through-life’, which is further decomposed into sub-claims described below.

Given the evolving nature of the generic E3S Case alongside the detailed design, some of the underpinning arguments and detailed evidence remain under development. The conclusions of the chapter therefore provide an evaluation of how the arguments and evidence presented, and their trajectory, provide confidence in the case achieving its objective at this stage.

[Sub-Claim 3.1.1] All credible Postulated Initiating Events (PIEs) for the RR SMR design are identified, fully defined and sentenced appropriately for analysis.

This is further decomposed into sub-claims [3] on hazard identification, sentencing and PIE definition for all types of faults, IH and EH induced failures, malicious attack induced failures, and accident scenarios. Arguments and evidence to underpin the claims is summarised in:

- Section 3.1.4, which summarises the PIEs relevant to the design.

- Sections 3.3 and 3.4, which describe the sentencing of IHs and EHs and approaches for their assessment.

[Sub-Claim 3.1.2] Measures are assigned to deliver the Fundamental Functions for all PIEs.

This is further decomposed into sub-claims [3] on assignment of safety, environmental, security and safeguards measures to deliver fundamental functions. Arguments and evidence to underpin the claims is summarised in:

- Sections 3.1.2 and 3.1.6 of the Chapter, which summarises the Fundamental Functions and the preventive, protective and mitigative measures to deliver them.
- Sections 3.3 and 3.4, which summarises the measures to ensure SSCs are protected against IHs and EHs.

[Sub-Claim 3.1.3] Measures that deliver Fundamental Functions are classified according to E3S significance of the functions they deliver.

Arguments and evidence to underpin the claim is summarised in:

- Section 3.2 of the chapter, which summarises the approach to E3S categorisation and classification and seismic performance classification.
- Section 3.0 (Appendix B), which presents a list of classifications assigned to SSCs.

[Sub-Claim 3.1.4] Measure design ensures Fundamental Functions are achieved through-life commensurate with their assigned E3S classification.

This is further decomposed into sub-claims [3] on SSC design to ensure delivery of allocated E3S functions through-life, covering allocation of E3S functional and non-functional system requirements, and the design definition of SSC to achieve them. Sub-claims also placed on operator actions to ensure delivery of E3S functions. Arguments and evidence to underpin the claims is summarised in:

- Section 3.1.7 of the chapter, which lists the E3S design requirements allocated to measures and SSC in accordance with their classification, and the approach to codes and standards selection.
- Section 3.1.8 describes the approach adopted for practical elimination of accidents that could lead to early or large radioactive releases.
- Sections 3.1.12, 3.9, and 3.10 describe the design approach to ageing management, verification of SSCs incorporating EQ, and EMIT respectively.

The claim is primarily covered in the systems engineering chapters 4 to 11, which presents the application of these design approaches to measures and SSCs. Claims that the metallic design of components ensures structural integrity proportionate to its safety classification are covered in E3S Case Tier 1, Chapter 23: Structural Integrity [4].

[Sub-Claim 3.1.5] Analysis demonstrates that Fundamental Functions are achieved for all plant states.

This is further decomposed into sub-claims [3] for each analysis topic. Arguments and evidence to underpin the claims is summarised in Section 3.1.9, which introduces the analysis approaches for deterministic safety, severe accidents, IHs and EHs, and PSA.

The claim is primarily covered in E3S Case Tier 1, Chapter 15: Safety Analysis [5], which presents the detailed methods and outputs of confirmatory analysis to demonstrate that the design can achieve the functions and meet relevant acceptance criteria.

[Sub-Claim 3.1.6] The overall plant implements suitable levels of DiD to deliver the Fundamental Functions.

Arguments and evidence to underpin the claim is summarised in Section 3.1.6, which summarises the relevant functions and measures across each level of DiD as defined in the Fault Schedule [6]. The claim is primarily covered through the overarching justification that risks are reduced to 'As Low As Reasonably Practicable' (ALARP), presented in E3S Case Tier 1, Chapter 24: ALARP Summary [7].

The proportionate summary of the arguments and evidence draws upon information in Tier 2 and Tier 3 documentation as presented in the E3S Case Route Map [3].

The route map for Chapter 3 decomposes further sub-claims from the top-level claim that are developed into CAE structures and evidenced within other chapters of the E3S Case, including:

- **[Sub-Claim 3.2]** The RR SMR chemistry regime and development of the chemistry systems design reduces risks during all normal operating modes and accident conditions for all phases of the lifecycle. This claim is covered in E3S Case Chapter Tier 1, Chapter 20: Chemistry [8].
- **[Sub-Claim 3.3]** The conventional and fire safety risks associated with the design, construction, commissioning, operation and decommissioning are identified, assessed, and mitigated to ALARP and comply with regulatory standards. This claim is covered in E3S Case Chapter Tier 1, Chapter 22: Conventional and Fire Safety [9].
- **[Sub-Claim 3.4]** The integration of Human Factors into the design minimises risks to humans to ALARP. This claim is covered in E3S Case Tier 1, Chapter 18: Human Factors Engineering [10].
- **[Sub-Claim 3.5]** Exposures of ionising radiation are reduced to ALARP throughout the lifecycle of the facility. This claim is covered in E3S Case Tier 1, Chapter 12: Radiation Protection [11].
- **[Sub-Claim 3.6]** The design facilitates development of operational arrangements in accordance with the E3S Case and associated defined limits and conditions. This claim is covered in E3S Case Tier 1, Chapter 13: Conduct of Operations [12] and E3S Case Tier 1, Chapter 16: Operational Limits and Conditions [13].
- **[Sub-Claim 3.7]** The commissioning programme supports as-built SSCs to achieve their E3S requirements. This claim is covered in E3S Case Tier 1, Chapter 14: Plant Construction and Commissioning [14].
- **[Sub-Claim 3.8]** The design facilitates safe decommissioning, with safety risks reduced to ALARP and using BAT for environmental protection'. This claim is covered in E3S Case Tier 1, Chapter 21: Decommissioning and End of Life Aspects [15].
- **[Sub-Claim 3.9]** The nuclear security arrangements for RR SMR will protect people and the environment from harm as a result of malicious actions which could result in unacceptable radiological consequences, the theft of nuclear material and/or the compromise of sensitive nuclear information. This claim is covered in E3S Case Tier 1, Chapter 32: Generic Security Report [16].
- **[Sub-Claim 3.10]** The RR SMR has been optimised through the application of BAT to prevent or, where not practicable, minimise the generation of radioactive wastes and discharges, to minimise the impacts on workers and members of the public. This claim is covered in E3S Case Tier 1, Chapter 11: Management of Radioactive Waste [17], Chapter 25: Minimisation of Radioactivity [18], Chapter 26: Sustainability [19], Chapter 27: Demonstration of Best Available Techniques [20], Chapter 28: Sampling and Monitoring Arrangements [21], Chapter 29: Quantification of Radioactive Waste Disposals [22], Chapter 30: Prospective Radiological Assessment [23], and Chapter 31: Conventional Environmental Impact and Other Environmental Regulations [24].

- **[Sub-Claim 3.11]** The design reduces risks and exposures to ALARP. This claim is covered in E3S Case Tier 1, Chapter 24: ALARP Summary [7].
- **[Sub-Claim 3.12]** The layout reduces risks during normal operation, faulted operation, and accident conditions where reasonably practicable. The site layout is described in E3S Case Tier 1, Chapter 1: Introduction [2]. The general plant layout principles and requirements for E3S are described within Section 3.1.7 this chapter. The claim on layout to reduce risks is further decomposed and evidenced across multiple chapters of the E3S Case, for example claims on the layout optimisation to minimise hazards is evidenced in E3S Case Tier 1, Chapter 15: Safety Analysis [5]. Further claims that the layout is implemented through the modular construction approach in the as-built plant are covered in E3S Case Tier 1, Chapter 14: Plant Construction and Commissioning [14].

3.1 General E3S Design Basis

3.1.1 E3S Objectives

3.1.1.1 E3S Fundamental Objective

The E3S fundamental objective is 'to protect people and the environment from harm'. Sources of harm may be either nuclear or conventional: nuclear considers harm that is postulated to occur from exposure to ionising radiation, whereas conventional considers all other postulated causes of harm.

The RR SMR is designed such that it can be constructed, commissioned, operated, maintained, and decommissioned to control and reduce risks from both nuclear and conventional sources of potential harm to levels that are ALARP, demonstrate application of BAT, and ensuring secure and safeguards by design.

3.1.1.2 E3S Design Principles

To achieve the E3S fundamental objective, a hierarchical decomposition of a set of E3S design principles have been established for RR SMR that provide a framework against which the design is evaluated and developed [1].

The E3S design principles are derived and justified based on an extensive and thorough desktop review of UK and international practices for nuclear facilities, including International Atomic Energy Agency (IAEA) suite of guidance for nuclear power plant design, Western European Nuclear Regulators' Association (WENRA) safety reference levels and guidance, The EUR Association's European Utility Requirements (EUR), Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) and Security Assessment Principles (SyAPs), and Environment Agency (EA) Regulatory Guidance.

Design principles for prevention to reduce risk associated with conventional health and safety are also applied to the RR SMR, in accordance with the Health and Safety at Work etc. Act 1974 (UK) [25], Council Directive 89/391/EEC – Occupational Safety and Health (Council of European Communities) [26], and their associated regulations.

3.1.2 E3S Functions

3.1.2.1 Safety Functions

The RR SMR is designed to achieve the three Fundamental Safety Functions (FSFs) set out in IAEA guidance, at all lifecycle stages. An additional 'fourth' FSF is also defined for RR SMR [1]. The four FSF are:

- Control of Reactivity (CoR).
- Control of Fuel Temperature (CoFT).
- Confinement of Radioactive Material (CoRM).
- Control of Radiation Exposure (CoRE).

A systematic approach is taken to identify those items important to safety that are necessary to fulfil the FSFs, described in the Hazard Identification and Production of the Fault Schedule Standard [27], summarised below:

- Undertake Hazard Identification (HAZID) workshops on safety measures and SSCs throughout the design process, to determine the mechanisms for how duty systems might fail, and how safety measures might be undermined in delivering their function.
- Group identified hazards accordingly within a hazard log [28] and use qualitative methods to sentence credible hazards that may lead to a radiological consequence, or determine if they may be screened out, for example, if they are inherently designed out or not applicable for the RR SMR.
- Group screened hazards to define PIEs, within the PIE definition report [29], considering fault sequence progression. PIEs are grouped into eight different categories based on the nature of the fault. Initiating Event Frequencies (IEFs) are calculated for each PIE on a best estimate basis. The list of PIEs is also reviewed to incorporate any further RGP for known Pressurised Water Reactor (PWR) faults.
    - The PIEs sentenced for RR SMR are described further in Section 3.1.4.
- Each PIE is carried forward into the Fault Schedule [6], which identifies High-Level Safety Functions (HLSFs) and appropriate safety measure defence. The number of safety measures is determined by IEF and potential unmitigated consequences of the PIE, in accordance with the categorisation and classification method (described in Section 3.2). To maximise usefulness, the Fault Schedule identifies HLSFs across all levels of DiD, including the functions that prevent, protect, and mitigate against design basis PIEs and Design Extension Conditions (DECs). These functions are aligned to each FSF to ensure they are maintained for a particular PIE. The Fault Schedule is accompanied by the safety measures table [30], which outlines HLSFs for each safety measure, and allocates safety categorised functional requirements onto the design of SSCs that comprise the safety measures – this includes any support systems such as emergency power supplies or the Heating, Ventilation and Air Conditioning (HVAC) systems. The Fault Schedule also interfaces with the (Control and Instrumentation) C&I engineering schedule [31], which provides the mapping of the trip parameters to individual faults for the specific safety measures. The allocation of safety requirements from the Fault Schedule through to SSC is managed through the RR SMR requirements management tool.
    - The safety measures to deliver the FSFs for PIEs are introduced in Sections 3.1.6.

Safety measures are defined as an SSC, or a combination of procedures, operator actions and SSCs, that deliver a HLSF to defend against a radiological consequence. Different combinations of SSC and operator actions may be demanded depending on the PIE it is protecting, therefore different ‘variants’ of the same safety measure are identified within the Fault Schedule [6].

The approach to EHs and IHs safety measures follows a similar approach but hazard identification is layout specific producing a hazard schedule, that then feeds into the fault schedule. Details of the approach EHs and IHs.

The systematic assessment, allocation and substantiation of operator actions is described further in E3S Case Tier 1, Chapter 18: Human Factors Engineering [10]. It is noted that the RR SMR is pursuing a passive design philosophy, which minimises reliance (where reasonably practicable) on operator actions, electrical power, and C&I systems, and rather relies on natural forces or phenomena such as gravity, pressure differences or natural heat convection.

3.1.2.2 Environmental Functions

The RR SMR is designed to deliver robust environmental protection. A key aspect of this is the identification of environmental measures that are required to perform a specific environmental function, which may be radiological or conventional.

The following Fundamental Environment Functions are identified for RR SMR:

- Elimination or reduction in the generation of radioactive waste.
- Minimisation of the volume and/or activity of radioactive wastes discharged or transferred to other premises.
- Minimisation of the impacts on the environment and/or members of the public of radioactive wastes discharged or transferred to other premises.
- Measurement and assessment of radioactive wastes discharged or transferred to other premises.
- Elimination or reduction of conventional environmental impacts.

The fundamental environmental functions are linked to BAT claims described in E3S Case Tier 1, Chapter 27: Demonstration of Best Available Techniques [20], with the exception of 'Measurement and assessment of radioactive wates discharged or transferred to other premises', which is linked to the claim in E3S Case Tier 1, Chapter 28: Sampling and Monitoring Arrangements [21].

SSCs to support BAT claims are identified through the BAT assessments, with those SSCs therefore contributing to a fundamental environment function linked to the corresponding claim. SSC contributing to Fundamental Environment Functions are designated as environmental measures and where applicable, Key Environmental Protection Equipment (KEPE) within those environmental measures are identified in accordance with the methodology described in Section 3.2.

Whilst many systems contribute to one or more fundamental environmental function, those that contain KEPE are primarily the waste systems and sampling and monitoring systems, including, but not limited to:

- Processing and Treatment System for Solid Radioactive Waste [KMA].
- Solid Radioactive Waste Storage System [KME].
- Liquid Radioactive Effluent Treatment System [KNF].
- Gaseous Radioactive Effluent Treatment System [KPL].
- Reactor Island HVAC System [KL].
- Auxiliary Sampling System [HUB].
- Hot Laboratory System [XRG].

The functions are evidenced through the Tier 2 design definition documents and associated Tier 3 design decision records, which are summarised in the relevant Tier 1 systems engineering chapters. This information is also used to support the arguments and evidence that underpin BAT claims [20] and presented in relevant environment-focused chapters.

3.1.2.3 Security Functions

For the generic design and case, security risks assessments are performed to influence the development of the design and provide confidence that the RR SMR will be Secure by Design (SbyD). Assessments include security analysis such as Vital Area Identification and Categorisation (VAI&C), layout design reviews, and other engineering engagements including design optioneering. The risk assessments prioritise the systems that present greatest security risk, to identify high-level protection requirements (Security Outcome and Postures) [16] and make recommendations for modification to engineering design or layout to reduce security risk. The outputs of the security risks assessments are documented, tracked and managed within the Risks, Assumptions, Issues, Dependencies and Opportunities (RAIDO) Log [32]. The high-level protection requirements are

developed as part of the Integrated Security System (ISS), at which point security functions are allocated to the relevant SSCs

A methodology for defining security functions has been established for the design of the RR SMR based on UK and international RGP [33]. This includes the definition of physical security functions that are delivered by the Physical Protection System (PPS):

- Deter – to discourage a potential threat actor from doing something by instilling doubt or fear of the consequences.
- Delay – provide a sufficiently robust design to permit a responding force to achieve the required outcome.
- Detect – systems and arrangements to alert a responding force to a potentially malicious or unauthorised act.
- Assess – systems and arrangements to enable a responding force to determine if an attack is underway and allow them to direct an effective response.
- Control of Access – systems and arrangements to ensure only authorised personnel can again access to restricted areas and protected assets.
- Insider Mitigation – process and arrangements to determine if a person is acting suspiciously or out of character, to allow immediate action to be taken or an investigation to be launched.

Cyber security functions are defined that are delivered by the Cyber Protection System (CPS):

- Identify – catalogues the software and hardware assets, identifies any potential vulnerabilities, determines the governance arrangements, commercial and regulatory environment, and identifies relevant threats and cyber security risks.
- Protect – implements appropriate measures to defend information systems and mitigate the risks identified in the Cyber Security Risk Assessment (CSRA).
- Detect – provides a timely indication of a potential cyber security incident.
- Respond – contains cyber security incidents, for example, by restricting connectivity to critical systems, bringing systems to safe states where this is appropriate, communicating the incident to responders and collecting evidence.
- Recover – restores systems and data, restores functionality and confidence in system performance, and prevents reoccurrence.

The functions are categorised and the SSC classified according to the methodology described in Section 3.2. The allocation of functions (AoFs) and security classification to security measure is undertaken as part of the ISS [34]. These functions are intended primarily for allocation to dedicated security measures.

The SbyD approach also identifies any engineering design or layout SSCs that could contribute to the ISS through the delivery of a security function. For example, potentially, any wall, door or other SSC providing physical segregation could be allocated the security function of ‘Delay’. This potential is identified, at a high level, as part of an initial SbyD assessment (carried out at the system level) which identifies whether an SSC should be the subject of a more detailed security assessment or could contribute to the ISS. Focus of initial SbyD assessment is on SSC with a Safety Class 1.

As the design of the PPS and CPS matures, SSCs are allocated security functional requirements as part of their Tier 2 Requirements Specifications. For example, if a door provides access to nuclear material, the security classification (and hence design requirement) will be higher than that for a standard door.

The security risk assessments and the application of security functions are described further in E3S Case Tier 1, Chapter 32: Generic Security Report [16].

3.1.2.4 Safeguards Functions

A key principle of the RR SMR is to ensure it is 'safeguards by design'. The generic E3S Case allocates non-functional system requirements onto the layout and SSC to enable the delivery of safeguards function, which will be specified in site-specific E3S Cases. For the example, aspects of the Reactor Island Control and Protection System [JY] will likely be allocated Nuclear Material Accountancy, Control and Safeguards (NMACS) functions.

3.1.3 Radiation Protection and Radiological Acceptance Criteria

3.1.3.1 Radiation Protection

The RR SMR is designed to protect against exposure to radiation and radioactive substances. The key element to the design approach is the adoption of the hierarchy of controls, where the means to minimise the exposure to radioactive material follows the International Commission on Radiological Protection (ICRP) justification, optimisation, and dose limitation model.

The hierarchy of controls is adapted and implemented in the design through optimisation of:

- Radiation shielding.
- Radioactive source term reduction.
- Dose management through engineered features and design to accommodate operational practices.

Shielding is implemented into the design throughout the reactor lifecycle, including primary shielding, secondary shielding, SSC shielding, radioactive material transport container shielding and refuelling process shielding. Guidance to shielding analysts and engineering teams throughout the major design phases is given through the Radiation Shielding Policy [35].

Radioactive sources are minimised through a structured approach, with focus on elimination, prohibition and substitution, localisation and minimisation, immobilisation, and mitigation. Guidance is given to engineers on these considerations within the design of measures through the Radioactive Source Term Policy [36].

Dose management principles to reduce dose are developed based on RGP and embedded into the design of the plant and layout. Focus is on the reduction of the source of radiation, increasing the distance between operators and the radiation source, decreasing the exposure time, and shielding the radiation source. Guidance is given to engineers though the Dose Management Policy [37], including regulatory requirements, dose targets for normal operations, dose targets under fault conditions, radiological designation of areas, minimisation of doses during maintenance, dose management during defuel and refuel, airborne contamination and decommissioning.

Additional design guidelines to implement these approaches [38] are used during design optioneering in line with the requirements of Ionising Radiations Regulations 2017 (IRR 2017), covering (but not limited to):

- Water chemistry and material selection optimisation.
- Use of labyrinths.
- Design of HVAC systems.

- Radiation and contamination zoning schemes to influence design of layout and HVAC configuration.
- Design of SSCs to facilitate decontamination and minimise deposition of activity.
- Control of access and egress to radiation-controlled areas, contamination-controlled areas, and high dose rate areas.
- Provision of installed and portable monitoring equipment.

The practical implementation of the hierarchy of controls supports the demonstration that any potential received doses are reduce to ALARP. The design, evaluation, and ALARP justification for radiation protection is summarised in E3S Case Tier 1, Chapter 12: Radiation Protection [11].

3.1.3.2 Radiological Acceptance Criteria

Numerical targets are used within the E3S analysis to evaluate the tolerability of risks and inform design decisions on where further design effort is needed. Dose/risk is evaluated against the numerical targets presented in

Table 3.1-1, which are based on the Basic Safety Levels (BSLs) and Basic Safety Objectives (BSOs) in the E3S design principles.

Two numerical target values for dose/risk are defined:

- A dose/risk target that shall be achieved by the design, defined as the boundary between tolerable and unacceptable, i.e. the BSL.
- A dose/risk target that the design should strive to achieve, defined as the boundary between broadly acceptable and tolerable, i.e. the BSO.

Irrespective of whether numerical targets are achieved, doses and risks are always controlled and reduced to ALARP. The design, evaluation, and ALARP justification for radiation protection is summarised in E3S Case Tier 1, Chapter 12: Radiation Protection [11].

Table 3.1-1: RR SMR Numerical Targets

Metric	Plant State	Shall be lower than (BSL)	Should be lower than (BSO)
Annual effective dose for any site worker that works with ionising radiation	Normal Operation	20 mSv	1 mSv
Annual effective dose for any site worker that does not work with ionising radiation		2 mSv	0.1 mSv
Average annual effective dose to defined groups of employees working with ionising radiation		10 mSv	0.5 mSv
Annual effective dose for any person off the site		1 mSv	0.02 mSv
Hourly dose rate to non-human species		N/A	40 µGy
Effective dose received by any person on-site arising from any single fault sequence within the design basis	Fault Conditions	20 mSv for IEF > 1E-03 pa 200 mSv for 1E-03 < IEF < 1E-04 pa 500 mSv for 1E-04 < IEF < 1E-05 pa	0.1 mSv
Effective dose received by any person off-site arising from any single fault sequence within the design basis		1 mSv for IEF > 1E-03 pa 10 mSv for 1E-03 < IEF < 1E-04 pa 100 mSv for 1E-04 < IEF < 1E-05 pa	0.01 mSv
Individual risk of death to a person on the site from accidents at the site resulting in exposure to ionising radiation	Accident Conditions	1E-04 pa	1E-06 pa
The predicted frequency of any single accident giving an effective dose to any person on-site, of: 2-20 mSv 20-200 mSv 200-2000 mSv >2000 mSv		 1E-01 pa 1E-02 pa 1E-03 pa 1E-04 pa	 1E-03 pa 1E-04 pa 1E-05 pa 1E-06 pa
Individual risk of death to a person off the site from accidents at the site resulting in exposure to ionising radiation		1E-04 pa	1E-06 pa
The predicted frequency of accidents giving an effective dose to any person off-site, of: 0.1-1 mSv 1-10 mSv 10-100 mSv 100-1000 mSv >1000 mSv		 1 pa 1E-01 pa 1E-02 pa 1E-03 pa 1E-04 pa	 1E-02 pa 1E-03 pa 1E-04 pa 1E-05 pa 1E-06 pa
The total risk of 100 or more fatalities from accidents at the site resulting in exposure to ionising radiation		1E-05 pa	1E-07 pa
Core Damage Frequency (CDF)		1E-05 pa	1E-07 pa
Large Release Frequency (LRF)		1E-06 pa	1E-08 pa

3.1.4 General Design Basis and Plant States

The general design basis for RR SMR includes the following plant states:

- Design Basis Conditions (DBCs):
  - DBC-1 (normal operation).
  - DBC-2i (normal operation, abnormal conditions).
  - DBC-2ii, DBC-3i, DBC-3ii, DBC-4 (fault conditions).
- DECs:
  - DEC-A (fault conditions).
  - DEC-B (accident conditions).

The objective of each plant state, the definition of the type of safety measure associated with each plant state, an estimate of the PIE frequency that is generally applicable, and the success criteria that safety measures must achieve, are presented in Table 3.1-2. It also aligns each plant state to levels of DiD (the approach to DiD is described further in Section 3.1.6).

The plant states listed in Table 3.1-2 incorporate UK RGP to define DBC frequent and infrequent faults at DiD level 3, defined as:

- Frequent faults: PIEs with an IEF exceeding 1 x 10^{-3}/yr. A minimum of two practicably independent and diverse safety measures are provided to deliver the success criteria for faults capable of resulting in severe accidents.
- Infrequent design basis faults: PIEs with an IEF between 1 x 10^{-3}/yr and 1 x 10^{-5}/yr. A minimum of one safety measure is provided to deliver the success criteria.

The approach also covers UK RGP for consideration of postulated frequent faults with failure of the first protective safety measure, which are considered within the design basis at DiD level 3 and not treated as DECs, as per the IAEA approach.

DECs are defined as:

- DEC-A: PIEs and complex sequences without fuel melt with an IEF less than 1 x 10^{-5}/year, and unmitigated consequences exceeding BSLs.
- DEC-B: Severe accident conditions postulated from the inherent hazard potential and from sequences arising from failures of duty, preventive, and protective safety measures.

IEFs and unmitigated consequences are used to determine if an initiating event is within or beyond the design basis. IEFs are calculated on a best estimate basis with the exception of natural hazards, where a conservative approach is adopted. Unmitigated dose consequences are determined on a conservative basis for design basis faults, and a best-estimate basis for DECs.

If an IEF is close to the boundary that defines the design basis, with data uncertainty or cliff-edge effects capable of having a significant impact on overall plant risk if the safety measure was moved between these two categories, then the bounding approach is taken, and the initiating event is assumed to be within the design basis.

For initiating events that do not have the unmitigated potential to give radiological consequences beyond those specified in Table 3.1-2, yet still give an appreciable dose, additional safety measures may be provided on probabilistic grounds to reduce risks to ALARP.

For postulated Initiating Events of Malicious Origin (IEMOs), the design basis is informed by the Design Basis Threat (DBT). The magnitude/capability of the DBT is included within the initiating event

definition, and not dependent on IEF. Security measures are defined using a graded approach to deliver security functions (see Section 3.1.2.3).

Environmental measures (and their KEPE) are defined to deliver environment functions dependent on the magnitude of the radiological impacts to people and the environment (see Section 3.1.2.2).

A systematic approach is taken to identify PIEs and IEFs, described in Section 3.1.2.1, which are characterised according to the postulated frequencies in Table 3.1-2.

The PIEs are then grouped into eight top level categories based on the nature of the fault and the types of demands they place on safety measures. Grouping and bounding is carried out by considering not only similar fault progression but also the severity of the fault, and the claimed safety measures. The eight PIE categories are:

- Intact Circuit Faults (ICFs) – faults which may lead to fuel melt but where the Reactor Coolant System (RCS) and connected systems remain intact.
- Loss of electrical supply faults – faults which are defined by a loss of electrical supply to multiple systems which, if unmitigated, may cause the simultaneous failure of multiple systems.
- Loss of Coolant Accidents (LOCAs) – faults which are defined by a loss of primary coolant from the RCS or connected systems.
- Fuel route and mechanical handling faults – faults which relate to the failure of mechanical handling equipment in containment and in the Spent Fuel Pool (SFP).
- Spent fuel faults – faults are related to the SFP systems and include intact circuit failures and loss of SFP coolant faults.
- IHs – defined as hazards that originate within the defined site boundary.
- EHs – defined as hazards that originate outside the defined site boundary.
- Non-fuel melt faults - non-reactor faults which lead to operator, or off-site, radiological dose but not from fuel melt events.

The PIEs are carried forward into the Fault Schedule [6] to identify HLSFs and allocate safety measure defence as described in Section 3.1.2.1. The PIE categories are also decomposed further to present more detailed bounding groupings for deterministic safety analysis, presented in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

The full list of PIEs, associated PIE category, and applicable operating modes, are listed in Section 3.14 (Appendix A).

Table 3.1-2: Plant States and Defence in Depth

DiD Level	Plant State	Plant State ID	Objective	Safety Measure		Postulated Frequency (/yr)		Success criteria Note 2
1	Design Basis Conditions (normal operation: desired conditions)	DBC-1	Prevention of abnormal operation and failures by design	Duty	Desired operating conditions	>1E-02	Note 1	<1 mSv /yr on-site radiation worker <0.1 mSv /yr on-site non-radiation worker <0.02 mSv /yr off-site No physical barriers breached where reasonably practicable
2	Design Basis Conditions (normal operation: abnormal conditions)	DBC-2i	Prevention of fault conditions and control of abnormal operation	Preventive	Minor deviation from desired operating conditions			
2	Design Basis Conditions (fault conditions)	DBC-2ii	Control of fault conditions within the design basis	Preventive	Frequent fault			<20 mSv on-site <1 mSv off-site No physical barriers breached where reasonably practicable
3		DBC-3i		Protective		1E-02 to 1E-03		
3		DBC-3ii			Infrequent fault	1E-03 to 1E-04		<200 mSv on-site <10 mSv off-site No more than limited relocation of radioactive material confined by at least one physical barrier
3		DBC-4				1E-04 to 1E-05		<500 mSv on-site <100 mSv off-site No more than limited relocation of radioactive material confined by at least one physical barrier
4	Design Extension Conditions (fault conditions)	DEC-A	Control of fault conditions beyond the design basis		Frequent fault and failure of the first protective measure	<1E-05	Note 1	<100 mSv off-site No more than limited relocation of radioactive material confined by at least one physical barrier
4	Design Extension Conditions (accident conditions)	DEC-B	Control of severe accidents	Mitigating				<100 mSv off-site At least one physical barrier intact confining any substantial relocation of radioactive material
5	N/A	N/A	Mitigation of radiological consequences of significant releases of radioactive material	Mitigating			Note 1	N/A

Note 1 – Plant state is not rigidly defined by its postulated frequency. While it is a reasonable estimate to expect that these plant states occur in the stated postulated frequency ranges, conditions postulated to occur outside of these ranges do not alter the alignment of the condition with the plant state.

Note 2 – Radiological success criteria for fault conditions are informed by ONR Target 4 Basic Safety Levels which set the minimum expectation in keeping with UK practice. Further numerical targets are defined which are used to drive dose and risk expectation for the design lower, recognising the overarching principle to reduce doses and risks to ALARP.

3.1.5 Prevention and Mitigation of Accidents

The approach to prevention and mitigation of accidents is through the application of the prevention principles and the implementation of DiD, described in Section 3.1.6. Mitigating measures (DiD level 4) are not regarded as a substitute for fault prevention (DiD levels 1 and 2) or protection (DiD level 3) barriers, but as further DiD. Conservative design and analysis, good operational practice, and adequate maintenance, testing and quality standards are specified to minimise the likelihood of faults. Priority is given to providing reliable and effective barriers (inherent features, equipment, and procedures earlier in the hierarchy) so that later barriers, though in place, need not be called upon. The design ensures that initiating events are defended against within the design basis and do not directly lead to DECs, where reasonably practicable.

3.1.6 Defence in Depth

3.1.6.1 Defence in Depth Approach

DiD against safety, security and environmental initiating events is 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.

To confine radioactive material, multiple physical barriers are in place between the reactor core and the environment, including the fuel matrix, fuel cladding, reactor circuit, and containment. Physical barriers are also provided for non-reactor locations confining radioactive material.

The integrity of the physical barriers is maintained through the provision of consecutive and practicably independent measures over five DiD levels, which deliver the FSFs and that would each have to fail before harmful effects could be caused to people or to the environment.

The alignment of DiD levels to plant states and associated success criteria for safety measures is presented in Table 3.1-2 based on the E3S design principles [1]. The five levels of DiD are adopted in accordance with UK and international RGP, including:

1. Safety Measures at DiD level 1 deliver duty safety functions to prevent abnormal operation and failures by design.
2. Safety Measures at DiD level 2 deliver preventive safety functions, which act to prevent a PIE, control abnormal operation, or prevent a demand on the protective DiD level 3 measure.
3. Safety Measures at DiD level 3 deliver protective safety functions, with both a principal and diverse means of delivering the FSF where appropriate for frequent faults, to control design basis faults and protect against escalation to an accident.
4. Safety Measures at DiD level 4 deliver mitigative DEC safety functions to control severe plant accident conditions in which the design basis may be exceeded, to protect against further fault escalation and mitigate the consequences of severe accidents.
5. Safety Measures at DiD level 5 deliver emergency response functions to mitigate radiological consequences of significant releases of radioactive material.

The RR SMR design approach is to ensure safety measures can deliver the FSFs across all levels of DiD, and to reduce the degree of functional dependence between them. Full independence is not possible, therefore, in accordance with RGP, the primary focus is to ensure independence between normal duty equipment provided in the design for operational purposes at DiD levels 1/2 and dedicated safety equipment provided in the design at DiD level 3, between the principal and diverse

protective safety measures at DiD level 3, and then between those protective safety measures and the mitigative safety measures at DiD level 4 for DEC-B.

3.1.6.2 Implementation of Defence in Depth Approach

3.1.6.2.1 Reactor

Control of Reactivity

The safety measures that deliver CoR for the reactor are:

- Duty safety measure: Duty Reactivity Control [JD04] by control rod insertion and withdrawal, and variation of primary coolant temperature.
- Preventive safety measure: Scram control rod release under gravity, initiated manually by an operator. Rapid Power Reduction [JD03] for turbine trip faults.
- Protective safety measure: Auto-Scram [JD01] control rod release under gravity, initiated using multiple trip parameters to provide full shutdown and reactivity hold down.
- Protective safety measure: A functionally diverse Alternative Shutdown Function (ASF) [JD02] to provide negative reactivity insertion through active pumped injection of potassium tetraborate into the core to provide full shutdown and reactivity hold down.
- Criticality during severe accidents is practically eliminated, subject to analysis (see Section 3.1.8).

Control of Fuel Temperature

The safety measures that deliver CoFT for the reactor are:

- Duty safety measure: Duty cooling chain.
- Preventive safety measure: High Temperature Heat Removal (HTHR) [JN03], with variants removing decay heat by:
    - Duty Condenser Decay Heat Removal (DHR), utilising the duty heatsink for normal condenser heat removal via the Main Cooling Water System (MCWS) [PA] mechanical draught cooling towers.
    - Condenser DHR heatsink cooling chain during fault conditions, including trip to house load following a LOOP, most ICFs and some LOCA faults, and full load rejection following turbine trip.
    - Active Atmospheric Steam Dump (ASD) [LBK50] to the atmosphere, via the Steam Generators (SGs) with pumped flow to the SGs from the Emergency Feedwater Supply System [LJ].
- Protective safety measure: Low Temperature Decay Heat Removal (LTDHR) [JN04] providing active decay heat removal during shutdown modes, using the Cold Shutdown Cooling System (CSCS) [JNA] and Essential Service Water System (ESWS) [PB] cooling towers.
- Protective safety measure: Passive Decay Heat Removal (PDHR) [JN02] removing decay heat from the core to the SGs via natural circulation in the RCS, with steam transferred from the SGs to dedicated heat exchangers that are cooled by the Local Ultimate Heatsink System (LUHS) [JNK] tanks of water, which boil-off to the atmosphere.
- Protective safety measure: Emergency Core Cooling (ECC) [JN01] removing decay heat through flood-up of the Reactor Pressure Vessel (RPV [JAA]) in a staged approach, including passive accumulator injection, gravity drain from a dedicated In-Containment Water Storage

System (IWSS) [JNH] tank, and containment sump water recirculation. The plant is depressurised through the high- and low-pressure Automatic Depressurisation System (ADS) [JNF]. Heat is released into containment and released to the atmosphere by the dedicated heat exchangers cooled by the LUHS [JNK].

- Protective safety measure: Fuel Pool Boil-Off (FPBO) [FA02] (variant 2) during refuelling operating mode 6a, when fuel is still in the core but ECC [JN01] is not available. The IWSS [JNH] provides a gravity-fed coolant supply to the RPV [JAA] to ensure fuel coverage for the first 24 hours, and the LUHS [JNK] provides coolant from 24 hours to 72 hours. The low-pressure ADS [JNF] lines are aligned to depressurise the RPV [JAA] by removing steam generated through boil-off, vented to the Containment Structure [UJA] and ultimately to the atmosphere through the Fuel Pool Venting System (FPVS) [FAN].
- Mitigative safety measure: Severe Accident Containment [JM02] utilising In-Vessel Retention (IVR) to provide heat removal from the molten corium that is retained in the RPV [JAA] during a core melt severe accident – see safety measures for CoRM below.

It is further noted that the Faulted Containment [JM01] safety measure provides containment isolation, which supports CoFT and successful operation of ECC [JN01], PDHR [JN02], and LTDHR [JN04].

Several of the CoFT safety measures that provide DiD share a dependency on the LUHS [JNK] as part of their cooling chain for the first 72 hours, noting the LUHS [JNK] are large and passive tanks with high reliability. Further independence and diversity of heatsinks is provided over the typical fault and accident sequence where these safety measures may be called upon. Notably, active SG cooling via Condenser DHR and ASD [LBK50] at DiD level 2, and the Active Containment Heat Removal that uses the CSCS [JNA] and ESWS [PB] at DiD level 4 for DEC-B accidents, which provide heatsink independence from the LUHS [JNK]. Further analysis of independence and diversity across the safety measures and the SSC that comprise them is presented in E3S Case Tier 1, Chapter 24: ALARP Summary [7].

Confinement or Radioactive Material

The safety measures that deliver CoRM for the reactor are:

- Duty and preventive safety measure: Duty Containment [JM03] and physical barriers of fuel clad, RCS and Containment.
- Protective safety measure: Faulted Containment [JM01], which delivers sub-functions:
    - Leak reduction through provision of a thick steel Containment Vessel (CV) that can withstand IHs, bounding pressures and temperatures, in addition to minimising the number of containment penetrations.
    - Containment isolation of fluid system penetrations and potential leak paths from the containment boundary, through the progressive and automatic closure of Containment Isolation Valves (CIVs).
    - Design basis hydrogen management to prevent hydrogen explosions and maintain containment integrity, implemented through the open free air volume of containment and the elimination of enclosed spaces within the containment layout, where practicable. A Hydrogen Reduction System (HRS) also utilises Passive Autocatalytic Recombiners (PARs) located within containment, which also incorporate a hydrogen monitoring subsystem.
    - Containment boundary monitoring to confirm conditions are within their operating range.

- Mitigative safety measure: Severe Accident Containment [JM02], which delivers sub-functions:
    - Severe Accident Depressurisation (SAD) to depressurise the primary circuit during DEC-B accidents and prevent high-pressure core melt sequences, manually initiated remotely. Two methods include the use of High Temperature Overpressure Protection (HTOP) valves within the Reactor Coolant Pressure Relief System [JEG], or the ADS [JNF] low pressure trains.
    - Hydrogen management to prevent hydrogen explosions and maintain containment integrity during severe accidents, implemented through the open free air volume of containment, and the elimination of enclosed spaces within the containment layout, where practicable. The HRS utilises PARs (as per the Faulted Containment [JM01] safety measure) in addition to hydrogen igniters located within containment, which also incorporates a hydrogen monitoring subsystem.
    - IVR to retain molten corium in the RPV [JAA] during a core melt severe accident. Flood-up of the RPV [JAA] cavity from the IWSS is initiated prior to core relocation through the Reactor Vessel Cavity Injection System (RVCIS), and as the corium cools steam is released into the containment atmosphere, either passively via the heat exchangers cooled by the LUHS [JNK] or actively using the CSCS [JNA] and ESWS [PB] cooling towers.
    - Containment isolation, required to initiate automatically by the Faulted Containment Safety Measure [JM01] for all severe accident sequences, noting manual isolation valve control is also available to the operator.
    - Active Containment Heat Removal, consisting of recirculation cooling or containment spray, which can be manually initiated to depressurise containment and reduce the pressure dependent leak rate to mitigate radiological consequences.

During Steam Generator Tube Rupture (SGTR) faults the PDHR [JN02] and ECC [JN01] also support CoRM to reduce the pressures in the primary and secondary circuits to terminate the release of primary coolant.

With the exception of hydrogen management and passive containment heat removal, all sub-functions of the Severe Accident Containment [JM02] safety measure are manually aligned by the operator. Operator actions will be captured in the Severe Accident Management Guidelines (SAMGs), which will be developed as described in E3S Case Tier 1, Chapter 13: Conduct of Operations [12].

Some major components such as the RPV [JAA] and primary circuit pipework support delivery of the FSFs across all levels of DiD. For these components, it is not considered reasonably practicable, or even possible, to provide independent DiD safety measures. As their structural failure would likely lead to catastrophic consequences that exceed DEC-B success criteria, they are assigned a Very High Reliability (VHR) safety classification (see Section 3.2) that requires a more stringent design approach, with their reliability demonstrated through a robust avoidance of fracture case. The components assigned VHR are listed in Section 3.0 (Appendix B). The specific design approaches and avoidance of fracture case is summarised in E3S Case Tier 1, Chapter 23: Structural Integrity [4].

Control of Radiation Exposure

The FSF of CoRE is delivered by radiation protection design safety measures during normal operations, including shielding provisions and appropriate zoning and access control. Shielding arrangements provide radiation protection during faults and accidents, in addition to operational safety measures that will prompt evacuation in response to alarms during fault and accident

conditions. Emergency Response and Plans (ERP) will mitigate the radiological consequences due to a release following an accident.

A simplified summary of the key safety measures that provide DiD for the reactor is presented in Table 3.1-3 based on the Fault Schedule [6].

3.1.6.2.2 Waste Systems

The safety measures that deliver CoRM for the waste systems are:

- Duty and preventive safety measure: Control and integrity of waste tanks and systems.
- Protective safety measure: Radiological bunds to contain leaks.

The FSF of CoRE is delivered by shielding provisions and appropriate zoning and access control, in addition to operational safety measures that will prompt evacuation in response to alarms during fault and accident conditions. ERPs will mitigate the radiological consequences due to a release following an accident.

3.1.6.2.3 Fuel Handling and Storage

Introduction

The fuel route for RR SMR covers fuel handling and storage, with operations including:

- New fuel import.
- Fuel storage and maintenance.
- Transfer of fuel between the fuel building and containment.
- In-containment refuelling activities, including core loading and Integrated Head Package (IHP) and RPV [JAA] internals lifts.
- Cask loading and export.
- Interim dry storage.

The FSFs of CoR, CoFT, CoRM and CoRE remain applicable across the fuel route operations, with some differences to reactor operations in the approaches to implement them:

- CoR is achieved through maintaining the sub-criticality of fuel whilst in transit and storage.
- CoFT is achieved through managing decay heat removal from spent fuel during transit and storage.
- CoRM is achieved through provision of appropriate storage structures and handling/lifting mechanisms for new and spent fuel to prevent or mitigate radioactive releases.
- CoRE is achieved through appropriate radiation shielding provisions, maintaining CoRM, and operational controls.

An overview of the key measures which implement FSFs across the levels of DiD for the fuel handling and storage systems is described below for each operation.

New Fuel Import

During import of new fuel, the FSF of CoR and CoRM is required, noting there is no decay heat to control. The design approach is to be developed for the transport containers but is anticipated to rely on the spacing and presence of neutron-absorbing material.

Following removal from the container, the New Fuel Store (NFS) will ensure spacing and neutron absorbers to maintain sub-criticality for duty and protective levels of DiD, implementing the Safe, Moderated, Absorbers, Unrodded, Geometry (SMAUG) [FA11] safety measure.

During lifting and loading operations, only one fuel assembly is lifted from containers at a time to maintain spacing, and control features on the overhead crane are anticipated to provide the preventative level of DiD against dropped load faults and ensure CoRM.

Fuel Storage and Maintenance

Spent fuel is stored in fuel racks within the SFP [FAB10], which contains sufficient water to ensure the fuel remains covered, shielded and cooled during normal and faulted conditions. The safety measures that maintain CoFT for spent fuel storage are:

- Duty and preventive measure: Duty Fuel Pool Cooling (FPC) [FA03] utilising active cooling trains that transfer heat from the pool to the atmosphere via a heat exchanger and pump, connected to the Component Cooling System (CCS) [KAA] and ESWS [PB] cooling chain.
- Protective measure: Faulted FPC [FA02] utilising the same cooling chain as the duty measure but with a diverse means of Alternating Current (AC) power supply and C&I provision, and additional redundancy of pumps and heat exchangers through cross-connects to the CSCS [JNA]. Automatic leak isolation is also incorporated.
- Protective measure: FPBO [FA01] utilising the mass of water present in the fuel pools to ensure the fuel assemblies remain covered following loss of active cooling. Water is heated and boils off to remove decay heat for at least 72 hours, with filtered venting via the FPVS [FAN]. Post 72 hours, active cooling can be restored, or alternative water supplies can be aligned. Automatic leak isolation is incorporated through passive features such as plugs and normally closed valves for inactive penetrations, and isolation valves for active penetrations.

The safety measures that deliver CoR for spent fuel storage are:

- Duty and protective measure: SMAUG [FA11] utilising spacing of fuel racks in the SFP and rack neutron absorbers to maintain sub-criticality of fuel assemblies during both duty and fault conditions.
- Duty and protective measure: Safe, Moderated, Unrodded, Geometry (SMUG) [FA12] for activities when fuel assemblies are outside the SFP rack neutron absorbers (for example, during cleaning or ex-core refuelling operations), the storage areas and handling systems will ensure separation to maintain sub-criticality of fuel assemblies both inside and outside containment. The design intent of SMUG is that any design basis misplaced/dropped load fault cannot result in criticality.

The safety measures that are anticipated to deliver CoRM for spent fuel storage include the civil structures and HVAC systems. The safety measures that deliver the CoRE for spent fuel storage include radiation shielding provided by the body of water and the pool structure, limitations on over-raise during spent fuel maintenance activities, HVAC systems, and alarms and evacuation procedures.

Transfer of Fuel

During refuelling, fuel is transferred between the fuelling block and the containment via the Fuel Transfer Channel [PT253]. The transfer systems are limited to only one fuel assembly at a time to maintain sub-criticality and deliver CoR.

The fuel pool cooling safety measures continue to provide CoFT during fuel transfer operations, and cooling is maintained within the transfer channel. The safety measures that deliver CoRM for spent fuel storage are anticipated to include the civil structures and HVAC systems.

The safety measures that deliver the CoRE during fuel transfer include radiation shielding provided by the body of water and the civil structures and HVAC systems. Access control safety measures will also be in place for temporarily high dose areas such as the fuel transfer channel inspection chamber.

In-Containment Refuelling

During refuelling operations, the IHP and RPV [JAA] upper internals are lifted by the polar crane to access the fuel assemblies. An inadvertent withdrawal of one or more control rods from the core during this operation could result in an unintentional criticality event.

The safety measures that deliver CoR during refuelling are:

- Duty and preventive measure: Rod Stay [FC12], whereby control rod withdrawal is prevented through duty claims on the Control Rod Drive Mechanisms (CRDMs), C&I decoupling, and guide pins to maintain even geometry.
- Protective measure: Polar Crane 'Ultimate' Trips and Interlocks [FC01], via trips on detector flux.

During refuelling a core misload fault could lead to a criticality event. Design features to prevent and protect against this fault are anticipated to include neutron monitoring, with administrative controls developed to support engineered controls.

During refuelling in operating mode 6b, the FPBO [FA01] provides CoFT.

Cask Loading and Export

Operations to load fuel and Non-Fuel Core Components (NFCCs) into dry storage casks are undertaken by a ground-based conveyance system, a specialised docking unit and the SFP Fuel Handling Machine (FHM). The fuel and NFCCs are loaded from the Cask Loading Pit (CLP) [FAB20] through the docking unit. The cask loading and export operations are being developed alongside selection of the casks supplier(s) to accommodate available cask designs and ensure delivery of the FSFs. The selection of the cask supplier(s) is outside the scope of the generic E3S Case.

Interim Dry Storage

Dry casks containing fuel and NFCCs are conveyed from the cask loading area to an external dry cask waste store. During storage, CoFT is maintained passively within the cask. CoR is maintained through geometric separation of fuel and fixed neutron absorbers within the casks, and the impact withstand of the cask itself noting that any activity is bounded by those where the cask is flooded as a moderator is present. The cask provides the final CoRM barrier after the fuel cladding. CoRE is delivered through shielding provided by the cask, and operational controls to be developed in the site-specific case.

Crane Operations

Within the SFP, the SFP overhead crane transfers new fuel from the transport container to the NFS and then on to the New Fuel Elevator (NFE). The NFE lowers the new fuel from the top to the bottom of the pool. The FHM then transfers the new fuel from the NFE to the fuel racks. Within containment, refuelling operations are performed by a polar crane (to lift the RPV [JAA] internals and IHP) and the in-containment FHM (to move fuel and NFCCs).

The polar crane and both FHMs are assigned a nuclear safety class 1 to ensure their reliability, such that their structural failure and potential for heavy dropped loads are considered as beyond design basis events. Design features for the polar crane include 'ultimate' trips and interlocks, such as brakes and hardwired C&I sensors on over-raise and over-speed.

Other mechanical handling systems within the fuelling block are assigned a lower safety classification. These systems are designed such that a dropped load cannot compromise an FSF. Furthermore, the fuel pool concrete structures are anticipated to be designed to withstand impacts from design basis failures of, or dropped loads from, lower safety classified handling systems.

3.1.6.2.4 Electrical, Control and Instrumentation

The safety measures allocate duty, preventive, protective and mitigative C&I functions to the C&I systems via the C&I Engineering Schedule [31]. The C&I architecture is designed with substantial DiD ensuring appropriate independence between the systems that deliver each function, implemented using a combination of physical separation, electrical isolation, and functional and communication independence. Independence is applied to prevent failures from systems of higher safety classification due to those of lower classification, and to prevent propagation of failures between redundant divisions within a system. The C&I systems that provide DiD include the:

- Reactor Protection Control System (RPCS) [JSA] to deliver C&I functions for duty and preventive safety measures.
- Diverse Protection System (DPS) [JQA], a hardwired system to deliver safety category A C&I functions for protective safety measures.
- Reactor Protection System (RPS) [JRA], a software-based system that provides a means to deliver safety category A C&I functions for protective safety measures, as well as the sole implementation of all safety category B functions for protective safety measures. Different variables are used where practicable. The RPS [JRA] are also responsible for post-accident monitoring functionality.
- Severe Accident Management System (SAMS) [JRQ] to deliver C&I functions for mitigative severe accident safety measures.

A conservative design approach is adopted for passive safety measures where practicable, however, active engineered safety measures are adopted for DiD and passive safety measures may require C&I actuation.

These safety measures allocate electrical load requirements to the electrical power systems in the RR SMR requirements management database. The electrical power systems adopt substantial DiD in accordance with RGP, incorporating design features such as house load capability and robust and reliable on-site standby AC power supplies. The electrical systems DiD approach includes the provision of the:

- Duty safety measure: Main Grid Connection [AC_].
- Preventive safety measure: Main Generator [MK_] to trip to house load operation if the main grid connection is lost. If unsuccessful, a transfer to the Standby Grid Connection [BC_] is possible without the need for load shedding.

- Protective safety measure: High Voltage (HV) Essential AC Standby Supply System [BD_] to supply essential loads following a loss of all grid connections i.e., Loss of Off-site Power (LOOP). Non-essential loads are shed, and power is supplied to the primary protective safety measures by two Diesel Generators (DGs). An Uninterruptible Power Supply (UPS) from batteries provides power for required C&I functions.
- Protective safety measure: Low Voltage (LV) Essential AC Alternate Supply System [BL_] to supply essential loads following a loss of the DGs combined with LOOP, i.e., a Station Blackout (SBO). The UPS remains available to supply power to C&I functions and actuation for both the secondary protective safety measures and the mitigative severe accident safety measures. Provision is also made for two alternate AC power sources.
- Mitigative safety measure: Provision of connection points to the LV Essential AC Alternate Supply System [BL_] and the HV Essential AC Standby Supply System [BD_] to allow for temporary mobile power sources.

The electrical systems provide 168 hours of autonomy for safety measures in accordance with the requirements in Section 3.1.7.3.

3.1.6.2.5 Summary

A simplified summary of the key safety measures that provide DiD for the reactor, waste systems and fuel handling and storage is presented in Table 3.1-3 and Table 3.1-4, based on the Fault Schedule [6].

Table 3.1-3: Overview of Defence in Depth for Reactor and Waste Safety Measures

<table>
<tr><th rowspan="2">FSF</th><th colspan="9">Defence in Depth Level / Indicative Plant State</th></tr>
<tr><th>DiD1</th><th colspan="3">DiD2</th><th colspan="3">DiD3</th><th colspan="2">DiD4</th><th>DiD5</th></tr>
<tr><th>DBC-1</th><th>DBC-2i</th><th colspan="2">DBC-2ii</th><th>DBC-3i</th><th>DBC-3ii</th><th>DBC4</th><th>DEC-A</th><th>DEC-B</th><th>n/a</th></tr>
<tr><td rowspan="2">CoR</td><td>Duty power control</td><td colspan="2">Manual Scram</td><td colspan="3">n/a</td><td>ASF</td><td>To be informed by analysis</td><td>To be informed by analysis</td><td rowspan="4">No measures reasonably practicable</td></tr>
<tr><td colspan="2">n/a</td><td colspan="5">Auto-Scram</td><td></td><td></td></tr>
<tr><td rowspan="2">CoFT</td><td>Duty Cooling Chain/ HTHR</td><td colspan="2">Faulted HTHR (Condenser DHR and ASD)</td><td colspan="4">PDHR</td><td rowspan="3">To be informed by analysis</td><td rowspan="3">Severe Accident Containment (including IVR)</td></tr>
<tr><td colspan="3">Duty LTDHR</td><td colspan="2">Faulted LTDHR</td><td>ECC / FPBO</td></tr>
<tr><td rowspan="2">CoRM</td><td colspan="3">Duty Containment</td><td colspan="4">Faulted Containment</td></tr>
<tr><td colspan="3">Control and Integrity of Waste</td><td colspan="3">Radiological Bunds</td><td colspan="3">No measures reasonably practicable</td></tr>
<tr><td>CoRE</td><td colspan="6">Shielding & Access Controls</td><td>Alarms and Evacuation</td><td colspan="2">No measures reasonably practicable</td><td>ERP</td></tr>
</table>

Table 3.1-4: Overview of Defence in Depth for Fuel Handling and Storage Safety Measures

<table>
<tr><td rowspan="2">FSF</td><td colspan="9">Defence in Depth Level / Indicative Plant State</td></tr>
<tr><td>DiD1</td><td colspan="2">DiD2</td><td colspan="3">DiD3</td><td colspan="2">DiD4</td><td>DiD5</td></tr>
<tr><td>DBC-1</td><td>DBC-2i</td><td colspan="2">DBC-2ii</td><td>DBC-3i</td><td>DBC-3ii</td><td>DBC4</td><td>DEC-A</td><td>DEC-B</td><td>n/a</td></tr>
<tr><td rowspan="3">CoR</td><td colspan="7">SMAUG</td><td>Practical Elimination</td><td rowspan="4">No measures reasonably practicable</td></tr>
<tr><td colspan="7">SMUG</td><td rowspan="2">Practical Elimination</td></tr>
<tr><td colspan="3">Rod Stay during Core Loading</td><td colspan="3">Polar Crane Trips on Neutron Flux</td><td>No measures reasonably practicable</td></tr>
<tr><td>CoFT</td><td colspan="3">Duty FPC</td><td colspan="2">Faulted FPC</td><td>Fuel-Pool Boil-Off</td><td>To be informed by analysis</td><td>No measures reasonably practicable</td></tr>
<tr><td>CoRM</td><td colspan="7">Physical barriers - Fuel Cladding / Container or Cask / Civil Structures / HVAC</td><td colspan="2" rowspan="2">No measures reasonably practicable</td></tr>
<tr><td>CoRE</td><td colspan="6">Shielding & Access Controls</td><td>Alarms and Evacuation</td><td>ERP</td></tr>
<tr><td>All</td><td colspan="7">Polar Crane and FHM Design Features</td><td colspan="3">No measures reasonably practicable</td></tr>
</table>

3.1.6.3 Presentation of Defence in Depth within the E3S Case

The Fault Schedule [6] provides a comprehensive tabulation of safety measures that deliver each of the four FSFs, aligned to PIEs across all operating modes. The Fault Schedule assigns HLSFs to the safety measures, and safety categorised functional requirements are allocated to the SSCs comprising the measures via the RR SMR requirements management system, which are reported in the Tier 2 Requirements Specifications for each SSC.

The design definition for safety measures and SSC to demonstrate they achieve their allocated safety categorised functional requirements is presented within the Tier 2 documents including System Design Descriptions (SDDs), Safety Measure Design Descriptions (SMDDs), and the Tier 3 design decision records. Verification and qualification evidence is presented within Tier 2 verification strategies and verification compliance reports, in accordance with the methods described in Section 3.9.

At Tier 1, E3S Case Tier 1, Chapter 6: Engineered Safety Features [39] provides a detailed summary of how the reactor safety measures and SSC that comprise them are designed and the verification activities to deliver their HLSFs, including the safety measure variations that deliver FSFs in response to different PIEs. E3S Case Tier 1, Chapter 9A: Auxiliary Systems [47] provides further detail for the fuel handling and storage measures. The supporting systems are also described in more detail as follows:

- Design of the reactor core and the fuel design that deliver FSFs is presented in E3S Case Tier 1, Chapter 4: Reactor (Fuel and Core) [70].
- Design of the RCS that contributes to delivery of the FSFs across all levels of DiD is described in E3S Case Tier 1, Chapter 5: Reactor Coolant System & Associated Systems [40].
- The architecture and systems that deliver the C&I functions for each safety measure are described in E3S Case Tier 1, Chapter 7: Instrumentation & Control [41].
- The electrical system architecture and systems that provide power to the active components and the C&I to initiate the safety measures, including the backup generation systems that supply power during LOOP and SBO, are described in E3S Case Tier 1, Chapter 8: Electrical Power [42].

- The cooling water and HVAC supporting systems and components that contribute to the delivery of the FSFs are described in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43].
- The civil structures that deliver FSFs are described in E3S Case Tier 1, Chapter 9B [44].
- The secondary circuit steam and condenser systems that contribute to the delivery of the FSFs are described in E3S Case Tier 1, Chapter 10: Steam and Power Conversion Systems [45].
- The waste systems and radiological bunds that deliver the FSFs of CoRM and CoRE are described in E3S Case Tier 1, Chapter 11: Management of Radioactive Waste [17].
- The radiation shielding provisions that deliver CoRE are described further in E3S Case Tier 1, Chapter 12: Radiation Protection [11].
- The ERPs that provide mitigation to deliver CoRE following an accident are described further in E3S Case Tier 1, Chapter 19: Emergency Preparedness and Response [46].
- The detailed performance analysis of safety measures against acceptance criteria is presented in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

The overarching demonstration that the safety measures and SSC across the levels of DiD reduce risks to ALARP is presented within the Tier 2 ALARP Summary Report [47] and summarised in E3S Case Tier, Chapter 24: ALARP Summary [7]. The overall justification that measures demonstrate BAT and are secure and safeguards by design is presented in (respectively) E3S Case Tier 1, Chapter 27: Demonstration of BAT [23], Chapter 32: Generic Security Report [20], and Chapter 33: Safeguards [29].

The design approach and protection measures for EHs and IHs to ensure delivery of the FSFs are summarised in Section 3.3 and 3.4 respectively.

3.1.7 Application of General Design Requirements and Technical Acceptance Criteria

3.1.7.1 Introduction

The plant, measures, and layout are designed to a set of deterministic principles to deliver their E3S functions and ensure a safe, secure, safeguarded, environmentally protected and sustainable design [1]. These principles and associated design approaches are described in the following subsections.

The principles are applied to the design through integrated E3S and engineering processes, specifically design optioneering [48] and the allocation of non-functional system design requirements to SSCs [49]. The design definition captures the design requirements and describes how they are achieved to ultimately demonstrate compliance with the principles. This design definition is presented within Tier 2 documents including Requirements Specifications, SDDs, SMDDs, and the Tier 3 design decision records.

The general design requirements applied to each SSC, and a summary of how the SSC design definition achieves them, is presented within the Tier 1 systems engineering chapters of the case.

3.1.7.2 General Design of Plant and Measures

The RR SMR employs design simplicity, prioritising inherent safety, security, environment, and safeguards protection. The hierarchy of controls is considered throughout the design optioneering process to eliminate risks in preference to controlling them. The waste hierarchy is also used to provide inherent environmental protection so far as is reasonably practicable, and to minimise the volume and activity of waste created and disposed using BAT.

Measures are conservatively designed to deliver their functionality in a passive manner with minimal reliance on control systems, active systems, or human intervention. Active engineered measures that are automatically or manually initiated, administrative measures and mitigative measures are also employed (with preference in that order) to contribute to levels of DiD and diversity. The passive and active measures are introduced in Sections 3.1.6.

All E3S measures that deliver functions and the SSC that comprise them are designed to the following design requirements:

- FSFs are delivered following design basis IHs, implemented through design of the layout with appropriate separation and segregation, and provision of hazard protection measures for credible IHs. The design approaches for IH protection are described further in Section 3.4.
- FSFs are delivered following EHs, primarily implemented through provision of engineered hazard protection measures including the Hazard Shield and Seismic Isolation System (SIS), which attenuate loads from hazards to ensure SSCs of high E3S classification can deliver their functions within limits for withstand. The design approaches and protection measures for EHs are described further in Section 3.3.
- Common Cause Failures (CCFs) are mitigated through inclusion of redundancy, diversity, and segregation within and between measures in a sequence, where reasonably practicable.
- Measures are highly reliable commensurate with safety classification, with a baseline probability of failure on demand for demand-based safety measures or failure frequency for continuously operating safety measures in line with Table 3.1-5.
- Human-Machine Interfaces (HMIs) are optimised for reliable human performance, through a consistent design approach in accordance with the HMI Style Guide [50], and AoF between human actions and engineered elements of a system.
- Equipment is qualified to deliver functions within their expected environmental, operating and seismic service conditions, through adoption of the approach to EQ presented in Section 3.9.
- Design codes and standards are commensurate with safety classification (see Section 3.1.7.6).
- Design and layout facilitates EMIT activities that ensure through-life reliability and performance.
- Installation, commissioning, and decommissioning are facilitated in accordance with the modularisation approach for build certainty and commissioning/decommissioning strategies.
- Decommissioning is facilitated by design of SSCs to reduce activation of materials, prevent or minimise buildup and spread of contamination, and reduced radioactive waste generation.
- Ageing and degradation processes are understood and managed (see Section 3.1.12). The design of SSCs ensures adequate margin between the intended operational life and the predicted safe working life, such that ageing and degradation processes do not threaten the delivery of FSFs during the operational life of the plant.

Measures are also designed to deliver their functions in accordance with specific deterministic principles that are assigned based on the safety classification of the measure, described in subsequent sections.

The overall plant is designed to ensure conventional safety. Conventional safety legislation and regulations are fully integrated within the Integrated Management System [51], rather than undertaken as auxiliary activities. Conventional safety assessments are performed at pertinent points during the design lifecycle to provide assurance and drive emergent requirements and RGP into the

design. Further details of risks assessments are provided in E3S Case Chapter Tier 1, Chapter 22: Conventional and Fire Safety [9].

Table 3.1-5: Safety Measure Failure Frequency or Probability

Safety Measure Classification	Failure Frequency (per year)	Probability of Failure on Demand
Safety Class 1	1E-03 to 1E-05	1E-03 to 1E-05
Safety Class 2	1E-02 to 1E-03	1E-02 to 1E-03
Safety Class 3	1E-01 to 1E-02	1E-01 to 1E-02

3.1.7.3 General Design of Safety Class 1 and 2 Measures

General Design

Safety class 1 and 2 measures are of high safety significance (see Section 3.2), and therefore SSCs comprising these measures are designed to stringent design requirements, including to deliver their functions:

- In the most onerous initial operating state within the inherent capacity of the facility permitted by the operating rules.
- Following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
- With segregation of redundant trains from one another.
- Without reliance on the correct performance of other equipment.
- In the presence of failures or unintended operation of other equipment, where this could exacerbate the consequences, or otherwise make the fault more severe.
- With diverse means of initiation between measures to the extent reasonably practicable, for sequences where both measures require automatic initiation.
- With a diverse on-site supply of essential services between measures, for sequences where both measures require the same essential service.
- Without reliance on operator action in the Main Control Room (MCR) within the first 30 minutes, or outside of the MCR within 1 hour. When this is not reasonably practicable, action outside the MCR within 1 hour can be accepted when personnel are already present in the locality of the place where actions are required and those actions are delivered through written procedure.
- Without reliance on essential services, including electrical and water supplies, from on-site mobile equipment for 72 hours or from off-site equipment for 168 hours, including during a LOOP and SBO.

Redundancy Levels and the Single Failure Criterion

Safety class 1 measures delivering safety category A functions are designed to further requirements to meet the single failure criterion. This includes sufficient redundancy/capacity within the SSCs that comprise the measures, where practicable, to demonstrate that following an initiating event, safety functions can be delivered in the presence of a single random failure.

The single failure criterion is defined as the most onerous single failure amongst all SSC essential to the success of the safety measure, including supporting systems such as electrical supply, HVAC or water tanks. In accordance with UK practice, both passive and active single failures are considered to occur from the start of the initiating event.

The design approach for redundancy of safety class 1 measures ensures either suitable provision within the SSC to account for outages of trains of systems or components for EMIT, or alternatively to mandate operational conditions for EMIT to be undertaken during modes where the demand on the safety measure is reduced or not present. The design approach also considers an IH or EH assumed to cause loss of SSC contributing to a safety measure, where this is a credible PIE. Exceptions to the single failure tolerance can be justified for massive, passive civil structures such as water storage tanks, noting redundancy is often incorporated (such as for the LUHS [JNK]) to ensure high levels of reliability.

Tolerance of the design to achieve the single failure criterion is not established as a deterministic design rule for safety class 2 (or safety class 3) safety measures, and rather redundancy is incorporated as needed on a case-by-case basis to meet the relevant safety measure design rules or to meet probabilistic risk targets. This approach is also taken for setting redundancy levels of lower safety classified systems that can have a train taken offline for EMIT.

In summary, the RR SMR design approach to redundancy and the single failure criterion follows RGP and the E3S design principles, which may drive safety measure redundancy as follows:

- A train to deliver the safety functionality.
- An additional train if a train can be lost due to the PIE itself.
- An additional train for single failure tolerance for safety class 1 measures.
- An additional train if a train needs to be taken offline for EMIT for safety class 1 measures.

All four points apply to RR SMR safety class 1 safety measures, which typically incorporate three redundant trains (N+2) and adopt an approach to conduct EMIT (point 4) during shutdown modes, when there are no demands for that safety measure functionality. Safety class 2 measures and safety class 3 mitigating (severe accident) systems typically incorporate two redundant trains (N+1) in accordance with points 1 and 2.

The level of redundancy incorporated into the design of safety measures is specified within the Tier 1 systems engineering chapters of the E3S Case. The modelling of single failures is presented within the deterministic analysis in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.1.7.4 General Design of DEC-A and DEC-B Measures

Measures and associated SSCs for DEC-A and DEC-B are designed to achieve their functions:

- Following failures consequential upon the initiating event, and failures expected to occur in combination with that initiating event arising from a common cause.
- With a supply of onsite essential services diverse from sources claimed for DBC where practicable, for sequences where the same essential service is needed for DEC functions and no onsite diversity exists for DBC.
- Without reliance on operator action in the MCR within the first 30 minutes, or outside of the MCR within 1 hour. When this is not reasonably practicable, action outside the MCR within 1 hour can be accepted when personnel are already present in the locality of the place where actions are required and those actions are delivered through written procedure.

- Without reliance on essential services supplied from onsite mobile equipment for 24 hours or from off-site for 168 hours, including during LOOP and SBO.

3.1.7.5 General Design of Plant Layout

The plant layout is designed to reduce risks during normal operation, faulted operation and accident conditions where reasonably practicable. To achieve this, the following general design principles are applied to the plant layout:

- Normal operational dose to workers is reduced through segregation of radiation sources from occupied spaces.
- The frequency of initiating events, in particular IHs and EHs, is minimised by segregation of potential hazard sources from classified SSCs and people.
- Access to site locations is controlled, including prevention of access by external malicious threat actors.
- Access and egress routes incorporate sufficient space to facilitate:
    - EMIT.
    - Actions in response to initiating events.
    - Emergency escape in response to initiating events.
    - Recovery actions and re-supply of essential stocks, material and equipment following an initiating event.
- Movement of nuclear matter is reduced to the extent reasonably practicable.
- Wastes and effluents are treated as close as possible to their place of production.
- Space provision is made for construction, assembly, installation, erection, and decommissioning.
- Space provision is made for equipment and services required for accident management and emergency response.

These general principles are decomposed into a more detailed set of E3S requirements and constraints to inform the plant layout development [52]. Requirements are also allocated from SSC to ensure sufficient space to implement their design within the overall layout. The layout is continuously informed by the iterative safety analysis performed on the layout, in particular the outcomes from IH and EH analysis, Lifecycle Risk Assessments (LRA) for conventional health and safety, and dose assessments, which also inform permanent and temporary shielding provisions within the layout.

All E3S (and non-E3S) requirements and analysis outputs are considered holistically within the layout design definition to reduce overall risks. This may require balances and compromises where not all requirements can be fully achieved, for example, physical contamination zoning barriers may need to be optimised to allow for emergency egress routes. The holistic considerations and justification of the layout design definition is presented within the Tier 2 Layout Summary Reports and associated Tier 3 design decision records. Arguments and evidence from these reports is used to underpin claims on the layout design, presented across Tier 1 chapters of the case as described in Section 3.0.3.

3.1.7.6 Codes and Standards

SSCs important to nuclear safety are designed, manufactured, installed, examined, and inspected using codes, specifications, and standards commensurate with their safety classification (see Section 3.2).

Safety class 1 and 2 SSCs are designed to appropriate nuclear industry-specific codes and standards, and safety class 3 SSCs may be designed to appropriate nuclear or non-nuclear specific codes and standards.

Codes and standards are selected and justified for the following:

- Mechanical components [53].
- Reactor Island mechanical handling equipment [54].
- C&I codes and standards [55].
- Electrical power system codes and standards [56].
- Civil and structural codes and standards [57] and aseismic bearing [58].

Competent persons are responsible for selecting the codes and standards to be used for their specific SSC. The selected codes and standards are to be captured within the Tier 2 Requirements Specifications for each SSC, including the rationale for selection, justification of their applicability and that they represent RGP.

An overview of the codes and standards selected for the design of safety (and non-safety) classified SSCs are presented within the introductory sections of the Tier 1 systems engineering chapters of the E3S Case.

3.1.7.7 Modularisation

The RR SMR adopts a 'build certainty' approach, which aims to provide high confidence in achieving the declared build schedule and costs. An enabler of the approach is the application of volume manufacturing processes, as opposed to the traditional 'stick-built' approach for large infrastructure projects. It is intended that dedicated factories will manufacture components and systems which are then assembled on site in the site factory.

Modularisation is a key enabler for build certainty. It integrates structural functionality whilst allowing components and systems to be efficiently grouped, packaged, tested, and transported to site for assembly. Close-coupled modules, each constructed using a 'Kit of Parts', create a configurable selection of components that can brought together to meet design and E3S requirements.

The Modular Kit of Parts (MKoP) system contains components such as primary frames, barriers, and interfaces between civil concrete floors and Mechanical, Electrical and Plumbing (MEP) modules. The Civils Kit of Parts (CKoP) contains components such as cellular retaining walls, aseismic bearing pedestals, and structural steelwork.

The design of the MKoP and CKoP is in accordance with the E3S design principles [1] to ensure their implementation supports the V&V of E3S functions. The E3S design principles are delivered by the MKoP and CKoP through the allocation and implementation of the general design requirements for plant, measures and layout, listed in Sections 3.1.7.2 to 3.1.7.5. For example, an MKoP barrier may be designed to implement E3S requirements for IH protection measures such as fire resistance, and radiation shielding to minimise dose rates.

3.1.8 Practical Elimination

The aim of the practical elimination concept is 'to complement the adequate implementation of DiD by a focused analysis of those conditions having the potential for unacceptable radiological consequences'. The onus of the practical elimination demonstration is to show that these conditions are either 'physically impossible' or demonstrated as having an 'extremely low likelihood' of occurrence with a 'high degree of confidence'. This will be achieved through deterministic and probabilistic argument [59].

The approach for demonstrating practical elimination of postulated event sequences or phenomena that could cause a large or early release of radioactive material is summarised as:

1. Step 1 – Identification of postulated event sequences/phenomena that could result in a large or early release, including those deemed physically impossible.
2. Step 2 – Identification and assessment of safety provisions within the design.
3. Step 3 – Analysis demonstration that postulated event sequences/phenomena that could lead to a large or early release are either:
    a. Physically impossible in the design due to inherent safety characteristics of the system or facility, or,
    b. Extremely unlikely (less than 1E-07 per year) to occur with a high degree of confidence.

The total frequency of all event sequences leading to the large or early release frequency shall be less than 1E-06 per year [1].

For those sequences that are not impossible by design there are two aspects to the practical elimination argument 'extremely unlikely to occur' and 'with a high degree of confidence'.

The 'extremely unlikely to occur' (i.e. having an extremely low likelihood of occurrence) aspect of practical elimination is supported by probabilistic arguments that will be used to substantiate the claim that postulated event sequences/phenomena that could result in a large or early release are practically eliminated. The results of the Level 2 PSA are used to demonstrate that frequency targets are met and the occurrence of severe accident phenomena and individual sequences that can result in a large or early release is less than 1E-07 per year or used to support ALARP arguments. The frequencies associated with Radiological Release Categories (RRCs) (as defined within the Level 2 PSA) are used to demonstrate that the practical elimination of large or early release target (< 1E-07 per year) for individual sequences is met; if associated RRC frequencies are below this target, this provides confirmation that individual sequences within the RRC are also below the target.

The 'with a high degree of confidence' aspect is supported by deterministic arguments and evidence from deterministic analysis. Severe accident phenomena and event sequences from the level 2 PSA that have the potential to result in a large or early release, are demonstrated as practically eliminated through the provision of design features and adequate layers of DiD. The results of safety assessments are used to confirm adequate margins of safety, which in combination with the design provision and layers of DiD, provide a 'high degree of confidence'. The emergency safety measure (DiD level 5) would be implemented where required to protect the public in the event of a severe accident, however this is not claimed as part of the demonstration of practical elimination. Operator actions are considered, including the means to detect the required action where this information is available (for example, high Core Exit Temperature (CET)).

The phenomena identified within the Severe Accident (SA) Phenomena Identification and Ranking Table [60], in addition to RGP [61], can be categorised into generic phenomena that are postulated as having the potential to result in a large or early release:

- Rupture of Large Component in the RCS.
- High Pressure Melt Ejection (HPME) and Direct Containment Heating (DCH).
- Fast Reactivity Insertion Accidents.
- Large Steam Explosions.
- Detonation of Combustible Gases.
- Containment Overpressure.
- Molten Corium Concrete Interaction (MCCI) - Basemat Penetration or Containment Bypass.
- Severe Accident with Containment Bypass.
- Significant Fuel Degradation in a Storage Fuel Pool.

Practical elimination of the following phenomenon is predominantly considered within the design basis:

- Rupture of Large Component in the RCS.
- Fast Reactivity Insertion Accidents.
- Severe Accident with Containment Bypass.
- Significant Fuel Degradation in a Storage Fuel Pool.

Practical elimination of the remaining phenomena is supported by the functions of the Severe Accident Containment [JM02] safety measure, introduced in Section 3.1.6. The phenomena and relevant prevention or mitigation functions for DEC-B are summarised in Table 3.1-6. The design of the Severe Accident Containment [JM02] safety measure to achieve its functions is presented in E3S Case Tier 1, Chapter 6: Engineered Safety Features [39].

The demonstration that relevant postulated event sequences and 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 [5]. An overview of the Severe Accident Analysis (SAA) (DEC-B) approach is presented in Section 3.1.9.2.2.

Table 3.1-6: Severe Accident Phenomena Considered within DEC-B

Severe Accident Phenomena	Unmitigated Progression	Severe Accident Containment [JM02] Safety Measure Function
HPME and DCH	Rapid accident progression increases pressure in the RCS, leading to RPV [JAA] failure with significant pressure differential to the containment atmosphere. Molten corium ejection as entrained particulates create excess pressure and temperature (DCH) that compromises containment. Corium ejection may also directly damage the containment barrier, creating a source term for radioactive aerosols to release to the environment, or generate additional hydrogen within containment.	SAD

Severe Accident Phenomena	Unmitigated Progression	Severe Accident Containment [JM02] Safety Measure Function
Hydrogen combustion	High concentrations of hydrogen within the containment produced during accident conditions may combust, deflagrate or detonate creating high pressure conditions that compromise containment.	HRS
Steam explosions	Rapid transition of water from liquid to vapour upon contact with surfaces that are at significantly higher temperatures than water's boiling point. Water boils rapidly leading to a rapid expansion, generating a pressure wave that increases more rapidly than pressure relief systems can vent, with sufficient energy to compromise the integrity of the RPV [JAA]. This may result in ex-vessel phenomena such as HPME or ex-vessel steam explosions that may compromise the containment.	SAD IVR
MCCI	Molten corium enters the reactor cavity upon failure of the RPV [JAA], penetrating the concrete basemat, causing direct damage to containment as well as producing non-condensable gases from the thermal decomposition of concrete, which pressurises the containment atmosphere.	IVR SAD
Containment overpressure	Containment pressure rises significantly, such as following a break in the RCS or non-condensable gas production during MCCI.	SAD IVR with Passive or Active Containment Heat Removal Containment Cooling and Spray

3.1.9 Safety Margins and the Avoidance of Cliff Edge Effects

3.1.9.1 Introduction

Safety analysis informs the design and provides assurance of the DiD approach described in Section 3.1.6. An overview of deterministic, severe accident and probabilistic analysis approaches are summarised below. The analysis approaches for external and IHs are described in Sections 3.3 and 3.4 respectively. The outputs of each analysis method are presented in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.1.9.2 Deterministic Safety Analysis

3.1.9.2.1 Design Basis Analysis

Deterministic performance analysis is used to assess fault sequences informed by the Fault Schedule, to provide high confidence that safety measures can achieve their HLSFs to prevent, protect or mitigate those faults. Fault sequences are modelled using validated computational codes on a best-estimate basis, combined with conservative assumptions such as application of single failure criterion. The outputs of the analysis are judged against technical acceptance criteria to confirm suitable safety margins, including (but not limited to) margins for Departure from Nucleate Boiling Ratio (DNBR), peak fuel clad temperature, and radiological dose targets.

The plant state (Table 3.1-2) is used to define the success criteria that must be met at each level of DiD for protection against each fault, noting more stringent acceptance criteria are specified for DBC-2ii and DBC-3i frequent faults than DBC-3ii and DBC-4 and DEC-A infrequent faults. Only safety measures that deliver safety category A and B functionality are credited with reducing sequence frequency required for moving through the DBC-2ii, DBC-3i, DBC-3ii and DBC-4 plant states.

The scope of the deterministic performance analysis includes all plant states to ensure the absence of “cliff-edge” effects for beyond design basis events. The timespan of the performance analysis extends to the point that the plant has achieved a stable, safe state.

The initial conditions and key parameters used in the performance analysis will also support definition and substantiation of Operational Limits and Conditions (OLCs).

The RR SMR deterministic safety methodologies [62] and design basis performance analysis methodology [63] provide further detail on the analysis approaches.

3.1.9.2.2 Severe Accident Analysis

The aims of SAA are to support the demonstration of ‘practical elimination’ of large or early releases of radioactive material to the environment through design. SAA allows demonstration that for applicable severe accident phenomena, DEC-B measures can either prevent or mitigate associated severe accident phenomena to protect the integrity of the final confinement barrier. It also supports the demonstration that there are no DEC-B (DiD Level 4) ‘cliff-edge’ effects in the safety analysis and supports EQ through definition of the safe operating envelope under DEC-B conditions.

SAA is performed on a best estimate basis, with realistic underpinning data and assumptions, transient analysis, accident progression and estimation of source terms. Accident progression behaviours are predominantly modelled using validated computer codes. As part of the deterministic analysis, DEC-B measures are modelled to demonstrate relevant acceptance criteria are achieved, such as containment integrity. The SAA evaluation is used to inform the design of DEC-B measures and their effectiveness in preventing or mitigating the identified phenomena and where the limits of their effectiveness are, to ultimately reduce risks to ALARP. This will continue as the analysis iterates with the detailed design. The Fault Schedule tabulates the DEC-B measures at DiD level 4 and safety categorised functional requirements are allocated to SSC that comprise them.

SAA interfaces closely with PSA, with the Plant Damage States (PDS) developed in the level 1 PSA providing the starting point to generate a set of severe accident progression behaviours that are analysed to study the impact of success and failure of associated systems. This analysis is in turn used as input to the level 2 PSA whereby postulated accident scenarios are mapped according to the success or failure of the base events.

Further SAA applications will be realised as the site-specific cases are developed, such as development of severe accident management strategies, guidelines and procedures, and off-site emergency planning activities.

Full details of the SAA strategy, approach, and maturity at this stage of design are presented in the Severe Accident Management Strategy [64], illustrated in Figure 3.1-1.

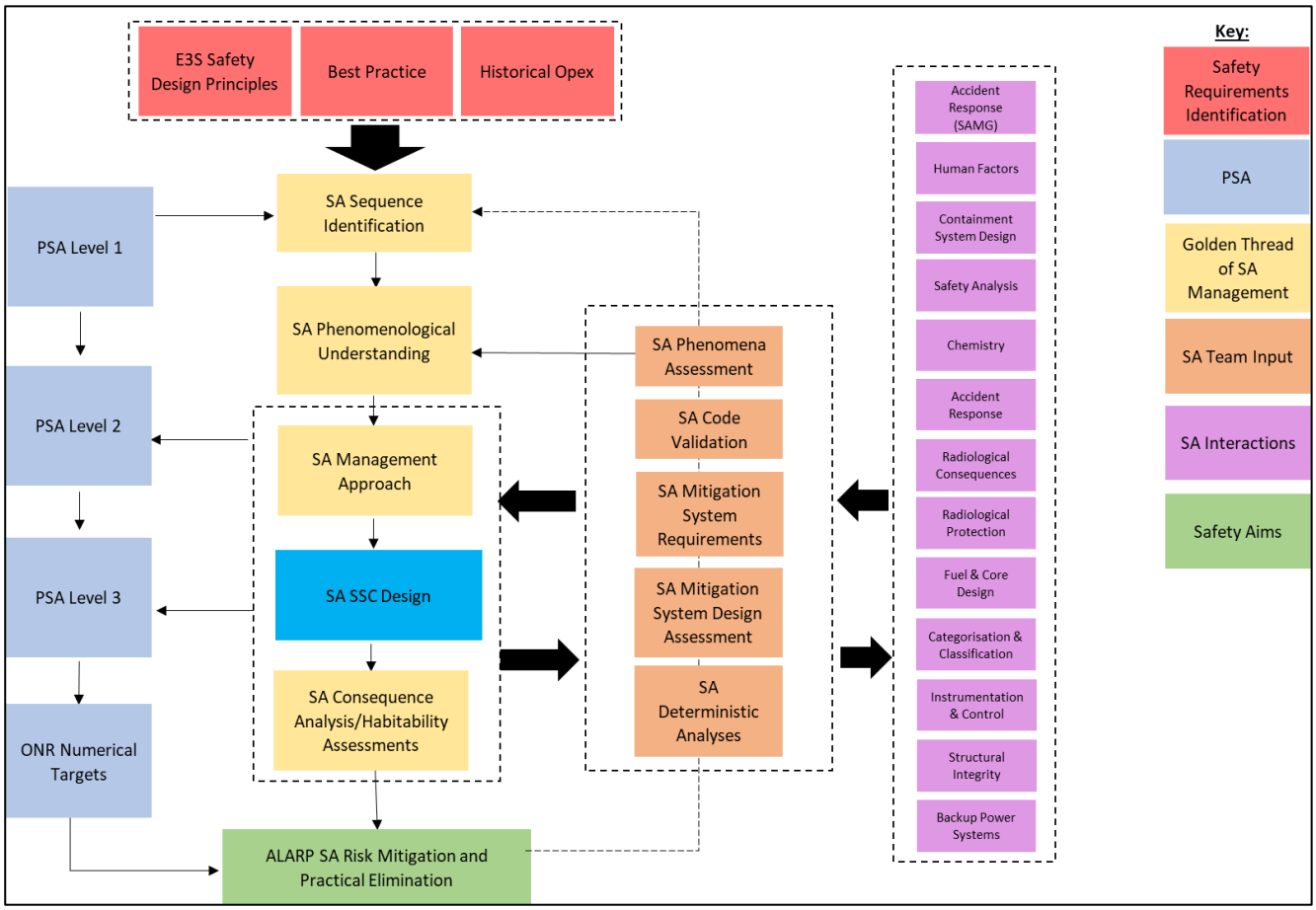


Figure 3.1-1: Severe Accident Analysis Strategy

3.1.9.3 Probabilistic Safety Assessment

PSA studies combine best-estimate IEF information with safety measure failure probability information, to evaluate the design against the numerical targets listed in Table 3.1-1, including:

- Comparison against the CDF target through a level 1 PSA.
- Comparison against the LRF through a level 1 and level 2 PSA.
- Comparison against the targets related to doses and numbers of fatalities through a level 1, 2 and 3 PSA.

The PSA models are constructed and iterated throughout the RR SMR design process, with the objective to:

- Study the benefits and detriments of various design options in support of risk minimisation.
- Evaluate risks to demonstrate they are below the numerical targets and are ALARP.

- Achieve a balanced and optimised design, so that no class of accident or feature of the design makes a disproportionate contribution to the overall risk.
- Input to standalone ALARP assessments outside of the design optioneering process, with quantitative assessment to support justifications.

Other PSA applications will continue to be realised as the RR SMR progresses throughout the plant lifecycle, such as the use of PSA to risk inform EMIT activities or OLCs. PSA has supported development of an overall EMIT strategy for RR SMR, described in Section 3.10.

Further details on the PSA strategy, approach, and maturity at this stage of design are presented in the PSA development strategy [65].

3.1.10 Design Approaches for the Reactor Core and for Fuel Storage

The reactor core, fuel handling and storage design approach to delivering FSFs is the same as the reactor design approach.

Hazard identification studies are undertaken and sentenced into PIEs, listed in Section 3.14 (Appendix A). The fault sequence progression is captured within the Fault Schedule [6] to identify HLSFs and safety measures are implemented across the levels of DiD, described in Section 3.1.6. Safety categorised functional requirements are allocated to the SSC that comprise the measures, which are designed to achieve the HLSFs in accordance with the design requirements described in Section 3.1.7.

3.1.11 Considerations of Interactions Between Multiple Units

The scope of the generic E3S Case considers a single unit only. It is noted the RR SMR E3S design principles [1] dictate that each unit of a multiple unit nuclear power plant should have its own independent measures. The possibility of one unit supporting another can be specified as far as this is not detrimental for safety, security or environmental protection.

3.1.12 Design Provisions for Ageing Management

The RR SMR has a 60-year design life, with some individual components required to demonstrate a longer lifetime to account for the commissioning and decommissioning processes. For the generic design and E3S Case, focus is given to proactive identification and minimisation of degradation mechanisms within the design of plant components, to ensure the structural integrity of plant components through life.

The relevant materials degradation mechanisms are identified using RGP and Operating Experience (OPEX), including IAEA, ONR Technical Assessment Guides (TAGs), United States (US) Nuclear Regulatory Commission (NRC) (in particular the Generic Ageing Lessons Learned (GALL) Report), and Electric Power Research Institute (EPRI) documentation. Additional focus is given to degradation mechanisms for any novel aspects of the design, such as the potassium hydroxide (KOH) primary chemistry, for which testing programmes are established to verify the performance of materials is no worse than typical PWR chemistry regimes.

The approach to justifying that the design is robust against ageing effects influenced by the design environment is set out in the RR SMR Ageing Management Plan (AMP) [66]. The AMP references to technical justifications that are generated for each degradation mechanism, which set out the arguments and evidence to underpin the claim that components are robust. Appropriate margins are provided in the design to account for degradation mechanisms.

The overall case for structural integrity of safety classified components is summarised in E3S Case Tier 1, Chapter 23: Structural Integrity [4]. The selection and justification of the RR SMR water chemistry is summarised in E3S Case Tier 1, Chapter 20: Chemistry [8].

For SSCs that cannot be designed for a 60-year design life, their replaceability is considered within the design and the plant layout.

3.1.13 Verification and Validation

The design undergoes robust Verification and Validation (V&V) to demonstrate evidence-based compliance with the requirements set, stakeholder needs, and demonstrate design intent, which include E3S requirements. This is set out in the RR SMR Approach to V&V [67].

The terminology used with respect to V&V is defined in line with industry standards and RGP as:

- Verification provides the objective evidence that a system, system element, or artifact fulfils its specified requirements and characteristics.
- Validation provides objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder needs and requirements, achieving its intended use in its intended operational environment.
- EQ is the generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements – approach to EQ is described in Section 3.9.
- Service conditions are the physical conditions prevailing or expected to prevail during the service life of an SSC, such as environmental conditions.

The V&V principles are to:

- Progressively build confidence in the design.
- Prove the design, making use of the requirements led approach to design, by focusing on design verification to assess design compliance with the requirements.
- Apply V&V to assess all attributes of the product with an underpinning priority of E3S.
- Achieve the establishment of EQ primarily through the design verification process, rather than by a separate process.

V&V activities are performed across design activities through the lifecycle, summarised below:

- Verification of E3S requirements through technical checking [49], and validation that E3S requirements meet E3S needs (allocated correctly and traceable).
- V&V of the design definition:
    - Verification that the design definition complies with its E3S design requirements and delivers its E3S functions [68]. This encompasses EQ to demonstrate that SSCs can deliver their E3S functions under the range of service conditions to which they might be exposed under different operational states, including fault and accident conditions.
    - Validation of the design definition is generally achieved through E3S requirements validation and design definition verification [67].
- Implemented solution:
    - Verification to demonstrate the completed solution complies with its design definition is achieved through manufacturing quality assurance. This shall be conducted in off-

site factories and/or onsite as the SSC is being installed/built, described further in E3S Case Tier 1, Chapter 14: Plant Construction and Commissioning [14].

- Validation of the implemented solution demonstrates that the implemented SSC, once manufactured / constructed, meets its design intent. This may be delivered in several steps through the implementation stage, building from components up to validation at a system and plant level following integration. The validation of the implemented solution is typically undertaken during the commissioning phase of the programme, though not always and may be undertaken earlier in the lifecycle.

The scope of the generic E3S Case includes V&V of E3S requirements and verification of the design definition to achieve E3S requirements.

V&V of requirements is achieved through the allocation and traceability of E3S requirements from their source, such as the safety analysis or E3S design principles. This is documented within Tier 2 requirement specifications for each SSC.

The scope of verification of the design definition applies to all SSC, including safety classified SSC, across all plant states. There are nine methods used for verification of the design definition, including:

1. Logical requirements decomposition, applied to E3S functional requirements whereby the E3S function can be deemed met if all associated non-functional performance requirements (constraints) are met.
2. Inspection, through visual checking of a design definition document or drawing.
3. Similarity, using comparable data sources from RGP or OPEX with sufficient contextual similarities.
4. Analysis, using verified and validated analytical techniques such as hand or software driven numerical calculations, simulations, or technical assessments.
5. Demonstration of functional performance using minimal or no instrumentation, such as trial fitting of a component.
6. Rig testing and recording of quantitative measurements, including industry-standard tests of custom-built applications.
7. Pre-Commissioning prior to final installation on site, such as within the module factory.
8. Commissioning onsite prior to entering service.
9. Operational testing and monitoring once in service.

The verification methods to verify E3S requirements are captured within Tier 2 verification strategies for each SSC, which also set out the sequence in which they should be completed, and the rationale for selection of specific methods.

Verification strategies will continue to develop into verification compliance reports as verification activities are conducted and evidence is generated, with reference to detailed verification evidence at Tier 3 such as test and analysis data.

Verification strategies and compliance evidence generated for SSCs are summarised and referenced within the Tier 1 systems engineering chapters 4 to 11 of the E3S Case. The structure for Verification reports within the E3S Case is illustrated in Figure 3.1-2.

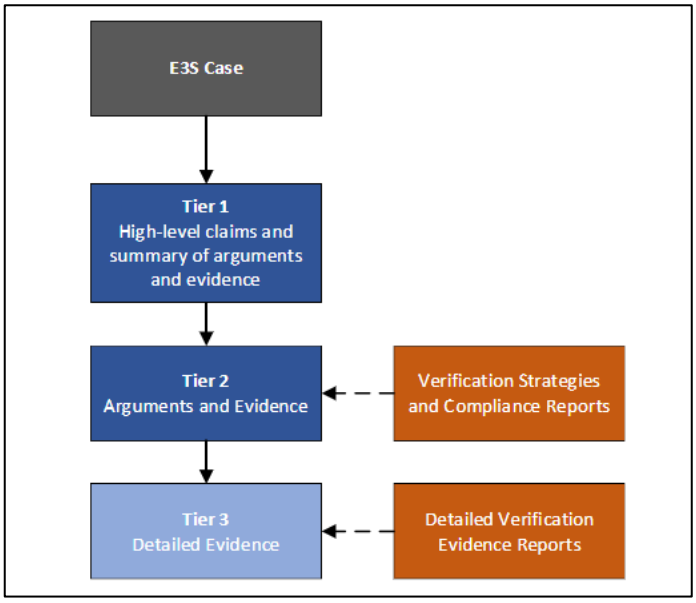


Figure 3.1-2: Verification Reports within the E3S Case Structure

The V&V programme is ongoing at DRP4, however the verification evidence presented in Version 3 of the E3S Case provides confidence that E3S classified SSCs can achieve their E3S requirement(s). The evidence comprises thermal hydraulic performance analysis and preliminary structural analysis to provide confidence that an SSC can achieve its safety categorised functional requirement(s) and meet its associated acceptance criteria, with a focus on safety class 1 and 2 SSCs. It also comprises inspection evidence that the design definition achieves its applicable E3S non-functional system requirements described in Section 3.1.7, for example, a requirement on an SSC to provide redundant trains to enable a train to be taken offline for EMIT.

3.2 Classification of Structures, Systems and Components

3.2.1 Safety Categorisation and Classification

DiD is achieved through the provision of multiple practicably independent safety measures that deliver the FSFs and terminate sequence progression, as described in Section 3.1.6. The function performed by each measure is assigned a category in accordance with its safety significance:

- Safety category A – any function that plays a principal role in ensuring nuclear safety.
- Safety category B – any function that makes a significant contribution to nuclear safety.
- Safety category C – any other function contributing to nuclear safety.

The categorisation assigned to each function is then used to classify the SSC that deliver the function. SSCs that deliver categorised functions are classified:

- Safety class 1 – any SSC that forms a principal means of fulfilling a safety category A function.
- Safety class 2 – any SSC that makes a significant contribution to fulfilling a safety category A function or forms a principal means of ensuring a safety category B function.
- Safety class 3 – any other SSC contributing to a categorised function.

Classifications determine the design requirements and codes and standards to which SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected, with more stringent standards required for higher classified SSCs. These design requirements and codes and standards are described further in Section 3.1.7.

The RR SMR safety categorisation and classification method and justification [69] has been developed based on RGP on assigning categorisations and classifications, including IAEA guidance, EUR, British Standards (BS EN 61226) and approaches adopted by other vendors within the UK regulatory environment.

The functions performed by safety measures over the various levels of DiD are assigned categories in accordance with Table 3.2-1, noting the table provides the minimum requirement. The functionality provided by any additional safety measures in the design is assigned to Category C.

A process of top-down decomposition cascades the assigned parent category to the functions performed by SSC in increasing levels of detail: functional groups of systems, sub-systems, components and sub-components. It is preferable to decompose the safety functions performed by SSC into as small a unit as usefully allows for assignment of different safety categorisations to different SSC parts.

Table 3.2-1: Safety Categorisation of the Functions Performed by Safety Measures over the Levels of Defence in Depth

Safety measure and its role in delivering Defence in Depth			Undefended Dose Consequence	>100mSv *off-site* / >500mSv *on-site*	10 - 100mSv *off-site* / 200-500mSv *on-site*	1 - 10mSv *off-site* / 20-200mSv *on-site*	0.1 - 1mSv *off-site* / 2-20mSv *on-site*	0.01 - 0.1mSv *off-site* / 0.1-2mSv *on-site*
Duty	Number of measures available to deliver Cat A or Cat B functionality in subsequent levels of DiD	0	when no subsequent functionality is available	**A** (VHR)	**A**	**A**	**B**	C
			when the subsequent functionality is Cat C	**A** (HR)				
		1		**B**	**B**	C (or B)	C	-
		2		C	C	C	-	-
Preventive and/or Protective #	Postulated preventive or protective measure demand frequency (per year)	>1E-01		**A+B**	**A+B**	**A** (+B, o)	**B**	C
		1E-01 – 1E-02		**A+B**	**A+B**	**A** (+B, o)	**B**	C
		1E-02 – 1E-03		**A+B**	**A** (+B)	**A** (+B, o)	C	-
		1E-03 – 1E-04		**A** (+B)	**A** (+B)	C	-	-
		1E-04 – 1E-05		**A** (+B)	C	C	-	-
		1E-05 – 1E-06		C	C	-	-	-
		1E-06 – 1E-07		C	-	-	-	-
		<1E-07		-	-	-	-	-
Mitigating				C	-	-	-	-

Notes to superscripts in table:

Where 2 measures are required and one delivers preventive functionality and the other protective functionality, then the preference should be to allocate the Cat A to protection.

HR / VHR – meaning (Very) High Reliability classifications.

(or B) - Where reasonably practicable, a Cat B measure should be provided.

(+B) - Where reasonably practicable, A+B should be provided.

(+B, o) - Where reasonably practicable, A+B should be provided, in particular for fault sequences where off-site risk considerations dominate.

-- - - The bold dotted line denotes the NT4 BSL, also called the design-basis region.

For EMIT and support functions, categorisations are assigned to one level lower than the function that is directly involved in delivering DiD. A categorisation refinement with time relationship is also described, with one categorisation level lower than the initial assignment required from 24 to 72 hours, and one level lower still from 72 to 168 hours. Lowering below a safety category C assignment, i.e. making an assignment of not categorised, is not permitted until the 168-hour mark, beyond which it is not categorised.

In general, safety category A functions are delivered by safety class 1 SSC, safety category B functions are delivered by safety class 2 SSC and safety category C functions are delivered by safety class 3 SSC, as summarised in Table 3.2-2.

Table 3.2-2: Safety Classification Method

Category	Classification
A	1
B	2
C	3

Where an SSC delivers several functions, its classification is assigned based on the highest categorised function it delivers. Equipment that does not deliver a categorised function is not assigned a classification, and an unclassified SSC is not tasked with delivering a categorised function. SSCs may perform several functions, and therefore it is possible for different parts of an item of an SSC to be assigned different classifications.

Up-rating of SSC classification beyond that required by Table 3.2-2 can be pursued when it is considered RGP, or where it is reasonably practicable to do so as an application of the preventive principle, or if SSCs are identified as important by the PSA.

In exceptional cases only a single level of DiD can be provided, i.e. there are no reasonably practicable safety measures that can be provided in the design in response to initiating events. Where no DiD is provided, certain catastrophic failure modes of an SSC could directly result unacceptable radiological consequences. In such cases, conceptual DiD shall be provided through assignment of a classification of an SSC that goes beyond the normal requirements for Class 1 and requires a more rigorous safety case, in terms of engineering substantiation, manufacturing controls, inspection, testing, quality assurance and through-life management.

There are two levels of classification beyond safety class 1, defined as follows:

- VHR: structural failure would lead to exceeding a DEC-B success criterion. It is not reasonably practicable to provide control of the resulting conditions either within or beyond the design basis.
- High Reliability (HR): structural failure would lead to exceeding a DBC-4 success criterion; however, DEC-A or DEC-B success criteria can be met. It is not reasonably practicable to provide control of the resulting conditions within the design basis; however, it is reasonably practicable to provide beyond design basis defence.

Where there is an interface between SSCs of differing classifications, the design incorporates engineered features as necessary to prevent the lower classified SSC having a negative impact on the higher classified SSC. Such features are included where credible failure modes are identified that warrants their inclusion. The feature that protects the higher classified SSC is assigned the same classification as the higher classified SSC.

The safety categorisation and classification for each SSC is presented throughout E3S Case Tier 1, Chapters 4 to 11. A list of the main SSCs important to E3S, together with their safety classification, are summarised in Section 3.0 (Appendix B).

3.2.2 Environmental Categorisation and Classification

Environmental measures are identified to fulfil Fundamental Environment Functions, as described in Section 3.1.2.2. Environmental measures are classified to determine their importance with respect to environmental protection in accordance with the environmental classification method [70].

An environmental classification does not dictate any additional requirements on that SSC, for example, the engineering standard to which it must be manufactured, installed, operated, maintained

etc., but rather it recognises that the SSC is required to perform an environment function. Optimisation of an environmentally classified SSC will be informed by BAT assessments and the capturing of functional system requirements.

Environmental measures could also be administrative actions placed onto humans; these will be captured in the RR SMR requirements management database against the relevant environmental function but are not assigned a classification. Administrative measures are developed as part of human factors design, including AoF to operators.

The SSCs that form the environmental measure are identified within the design definition information as KEPE and summarised in the relevant Tier 1 systems engineering chapters 4 to 11 of the E3S Case. A list of the main SSCs important to E3S, together with their environmental classification, are summarised in Section 3.0 (Appendix B).

3.2.3 Security Categorisation and Classification

Security functions are captured for the RR SMR design and aligned to the stages of a potential adversary activity, as described in Section 3.1.2.3. A graded approach to the design of protection systems that fulfil security functions is adopted to ensure the design of security protection is proportionate, with security functions assigned a security category.

Security categories are assigned based on potential consequences, in accordance with the methodology for categorisation and classification of security functions [33]. Security analyses are undertaken to identify the consequence level, including VAI&C, Categorisation for Theft (CfT), and CSRA. The consequence level obtained from these analyses is used to determine the required security outcome and posture using the tables in the SyAPs classified annexes [71].

Three security categories may be assigned:

- Category A: functions that play a principal role in achieving the desired security outcome, where failure would directly lead to the most severe consequences. Functions assigned this category are expected to provide continuous or immediate protection by directly interrupting an attack scenario, and to maintain their effectiveness when exposed to threat capabilities.
- Category B: functions that play a complementary role to security category A functions in achieving the desired security outcome, or functions that play a principal role where their failure would lead to less severe consequences than for category A functions.
- Category C: functions that play a complementary role to security category B functions in achieving the desired security outcome, or functions that play a principal role in achieving a baseline level of security in accordance with the desired security outcome.

Three security classifications are defined for the SSCs delivering security functions, according to the most significant security function allocated to it. For components, the contribution of the component in delivering the function shall also be considered when classifying the component, as not all components of the SSC will be critical in delivering the function. Table 3.2-3 provides guidance for classifying SSCs according to these factors.

Table 3.2-3: Security Classification of SSCs or Components Delivering Functional Security Requirements

		Contribution of the SSC or Component to Meeting the Functional Security Requirement		
		System or structure, or the component is the principal or sole means of meeting the requirement	The component makes a significant contribution to meeting the requirement	The component makes a minor contribution to meeting the requirement
Security Functional Category	A	Class 1	Class 2	Class 3
	B	Class 2	Class 3	Class 3
	C	Class 3	Class 3	Class 3

Quality and performance requirements can then be defined and recorded in the requirements management database according to the security classification of the SSC, in line with the following principles:

- Security class 1 SSCs shall have the most stringent quality requirements, and security class 3 SSCs the least.
- Security class 1 SSCs shall have the most demanding performance requirements, i.e., effectiveness and availability, and security class 3 SSCs the least.
- Security class 1 SSCs shall have the most significant anti-tamper requirements, and security class 3 SSCs the least.
- Security class 1 SSCs shall have the most significant supply chain security requirements, and security class 3 the least.
- Security class 1 SSCs shall have the most thorough through-life assurance requirements, and security class 3 the least.

The security categorisation and classification for each SSC is presented throughout E3S Case Tier 1, Chapters 4 to 11. A list of the main SSCs important to E3S, together with their security classification, are summarised in Section 3.0 (Appendix B).

3.2.4 Safeguards Categorisation and Classification

All SSCs required to deliver the safeguards functions shall be classified throughout the design phase.

3.2.5 Seismic Classification

Seismic performance classification defines the quality requirements placed on SSC and the required withstand capability of each SSC in response to seismic events. SSC which are important to, or may impact safety categorised functional requirements in the event of an earthquake are broadly classified:

- Seismic Performance Class 1 (SPC1) - any SSC which has an important safety categorised functional requirement in response to a seismic event within or beyond the design basis. SSC is to remain fully functional during and after a Design Basis Earthquake (DBE).
- Seismic Performance Class 2 (SPC2) - any SSC which unmitigated could have an undesirable impact on a seismic performance class 1 SSC or the long-term management of a seismic event within or beyond the design basis. SSC is to retain limited functionality during and after a DBE.
- Seismic Performance Class 3 (SPC3) - all other SSC. No seismic withstand requirements are defined for SPC3 SSC with respect to the DBE. However, all SSC are to be unaffected by repeated ground motion at the Operating Basis Earthquake (OBE) level.

The RR SMR seismic performance classification method [72] has been developed based on RGP to assign seismic performance classification in line with IAEA guidance, EUR and approaches adopted by other vendors within the UK regulatory environment.

The RR SMR definitions for DBE and OBE are developed in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73]. The seismic performance classification method is summarised in Table 3.2-4.

Table 3.2-4: Relationship between SSC E3S Classification and Seismic Performance Classification

SSC E3S Classification	SSC Seismic Performance Classification
1	SPC1
2	SPC1
3	SPC1 – for mitigating safety measures against severe accidents; or SSC which contribute to the delivery of category A safety functions beyond 72 hours after the occurrence of a DBE SPC2 - for SSC that may have unacceptable interaction with SPC1 SSC in case of DBE; or SSC relating to infrastructure needed for implementation of an emergency evacuation plan SPC3 – for all other SSC
Not classified	SPC3

Whilst it is the required response of an SSC to the DBE that defines its SPC, adequate margin to beyond design basis events with regards to cliff-edge effects are demonstrated through seismic margin assessments or PSA of earthquake severity.

The seismic categorisation and classification for each SSC is presented throughout E3S Case Tier 1, Chapters 4 to 11. A list of the main SSCs important to E3S, together with their seismic classification, are summarised in Section 3.0 (Appendix B).

3.3 Protection against External Hazards

3.3.1 Introduction

EHs are defined as those natural or man-made hazards to a site and facilities that originate externally to both the site and its processes. As EHs are beyond the control of the licensee, unlike for IHs, they cannot be eliminated through design.

This section provides a list of EHs (both individual hazards and reasonably expected combinations of hazards) considered in the design of the RR SMR. It also provides supporting information to give confidence that the FSFs will be adequately maintained both during and post EH events.

3.3.2 Principles of External Hazard Protection

The principle of EH protection is that duty systems will, with the exception of a loss of site services (for example, grid supplies), continue to operate during/post EHs up to their operating basis severity. The requirement for plant shutdown in the event of a non-negligible interruption to off-site supplies, whose failure is calculated to occur at a frequency significantly higher than the OB frequency, may be accepted.

For EHs beyond (i.e. more severe than) the operating basis event, it is conservatively assumed that there is a failure of one or more duty systems, requiring that the reactor be shut down and alternative cooldown initiated. The deterministic target is, therefore, that the safety measures that maintain the FSFs of CoR, CoFT, CoRM and CoRE withstand the relevant events to a defined severity.

The deterministic targets against EHs are achieved, therefore, if:

- For frequent EHs (>1E-3/yr), safety measures affording a safety category A or B function remain available.
- For infrequent EHs (≤1E-3/yr), safety measures affording a safety category A function remain available.

This includes the consideration of safety functions that support safety category A or B functions but are categorised using the 'categorisation refinement with time' approach outlined in Section 3.2.

EHs are defined at their design basis [74] and operating basis [75] severities. Therefore, the demonstration that the design achieves protection against EHs is through the following, as depicted in Figure 3.3-1:

- SSCs supporting a safety category A safety function shall be qualified to withstand EHs up to their design basis severity, with additional margins assessment to provide confidence in the absence of any cliff-edge effects.
- SSCs supporting a safety category B safety function shall be qualified to withstand frequent EHs up to their maximum associated severity. As, however, only operating and design basis severities have been defined, these SSCs are to be qualified against the design basis severity, thus achieving additional hazard resilience for infrequent faults.
- There is argued to be no requirement to qualify SSCs supporting safety category C design basis safety functions against operating basis EHs, as the application of suitable codes and standards should achieve the aspired level of resilience. Furthermore, even if a failure were to occur because of a less severe EHs than the operating basis event, the deterministic targets would still be achieved.

The last bullet above excludes severe accident measures that are employed under DECs, which are required to deliver their function following design basis EHs.

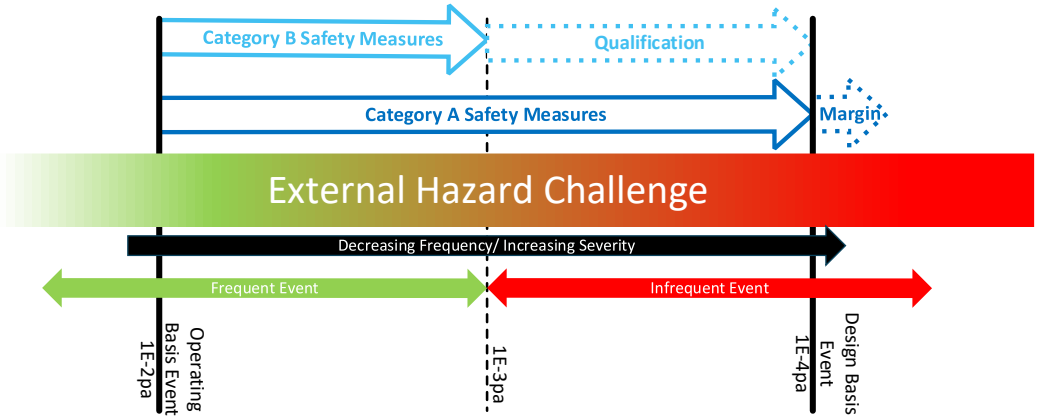


Figure 3.3-1: Hazard Qualification of Non-Discrete External Hazards

3.3.3 Approach to External Hazards Assessment

3.3.3.1 Introduction

The EH strategy contains the high-level approach for EH assessment for the RR SMR [76]. The objective of the EHs topic area is to identify EHs that have the potential to affect nuclear safety, characterise these hazards appropriately and provide input to the design to ensure that safety is maintained both during and after the EH event.

Hence, the approach to EH assessment includes the:

- Identification of EHs.
- Screening of EHs.
- Definition of reasonably foreseeable combinations of EHs.
- Characterisation of EHs (for example, severity, frequency).
- Designation of design basis consequential his.
- Optioneering to achieve safety measure resilience to the above hazard challenges.

3.3.3.2 External Hazards

The EHs are considered based on reviews of RGP, Great Britain (GB) and International Regulatory Guidance and internal sources [74], and introduced in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73]. The EHs are:

- Air Temperature.
- Relative Humidity.
- Wind.
- Wind-Driven Missiles.
- Tornado.
- Tornadic Missiles.

- Rainfall.
- Hail, Snow and Sleet.
- Ice.
- Cooling Water Temperature.
- Seismic.
- Accidental Aircraft Crash (AAC).
- Lightning.
- Volcanic Ash*.
- Sand and Dust*.
- External Atmospheric Pressure.
- Space Weather.
- Industrial Hazards*.
- Electromagnetic Interference (EMI)*.
- Flooding (pluvial).
- Flooding (other sources, for example, fluvial)*.
- Biological Phenomena.
- Drought.
- Geological*.
- Landscape Change*.
- Natural Fire*.
- Loss of Off-site Power.
- Loss of Off-site Water (LOOW).

Those hazards marked with an '*' represent site-specific hazards that can only be quantified once a location has been specified. These have been screened from consideration at the onset of the EHs assessment for the generic design. General comments providing reassurance on their assessment and mitigation, in addition to bounding values where practical, are provided in the Generic Site Envelope (GSE) [74].

The representative GSE, within which the plant is designed to operate safely, is defined to facilitate deployment of the RR SMR in a range of potential locations. For most cases, a design basis has been established which bounds the GB values. Climate change adjustment factors are calculated using the UK Climate Projections 2018 (UKCP18) [77]. Hazard values and further information on the generic site characteristics can be found both in the GSE and in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73].

An assessment of the site-specific factors excluded from the GB GSE is captured as a commitment on the future dutyholder/licensee/permit holder in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73]. Identification and assessment of site-specific hazards shall be undertaken at the site licensing and permissioning stages by the future dutyholder/licensee/permit holder.

A comparison of site-specific data against the GB GSE shall also be undertaken to confirm that the justification of EHs provided for the generic design remains suitably bounding for the specific site.

Where this is not the case, further assessment may be required. This is captured as a commitment to the future dutyholder/licensee/permit holder in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73].

3.3.3.3 Combinations of External Hazards

Assuring resilience against EHs requires the consideration of multiple hazards. These combinations of hazards may occur simultaneously, as a result of a shared initiating event (for example, meteorologically induced effects), or as a result of their frequency of occurrence being such that their simultaneous occurrence is deemed to be within the design basis. Hazard combinations are defined as:

- Correlated Hazards: An EH that may occur simultaneously with the primary hazard because both depend on a common physical process (for example, wind and rain).
- Consequential Hazards: Hazards (Internal and External) that are the derived effects of primary, correlated and secondary hazards and or their typical effects (for example, rain and flood).
- Coincidental/Independent Hazards: Realistic combinations of randomly occurring independent EH affecting the site simultaneously (for example, earthquake and air temperature hazards). These hazards are not correlated through a physical process but could occur at the same time.

The identification and analysis of credible combinations of EHs for the RR SMR is provided in the Combined External Hazards Report [78], as outlined in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73]. From this analysis, further grouping of hazards has been undertaken according to those events that provide a cumulative engineered effect (i.e. afford an equivalent engineering challenge) that may be reasonably expected to occur at the same time [79]. The aim of this exercise was to sub-divide hazard scenarios into engineering challenges in support of ongoing design development, whilst applying a proportionate approach to the consideration of EH combinations.

EH challenges consider both correlated hazards originating from a common cause, as well as reasonably foreseeable independent EHs likely to occur simultaneously and exert additional loadings. For example, meteorological conditions such as wind occurring independently to but at the same time as a seismic event. The associated hazard severities for each EH occurring within a challenge are provided, together with the rationale in the External Hazard Challenge Report [79]. A proportionate approach is applied when considering the combined hazard loadings considered in a challenge, to consider reasonably foreseeable combinations of hazards whilst avoiding unnecessary over conservatism.

The following sections present the grouped ‘EH challenge’ and outline the approach to hazard protection for each of the challenges. When considering combinations of external/IHs, EHs are assumed to be the primary hazard in the sequence, noting that man-made EHs have been screened out on the basis of being site-specific. The External-Internal Combined Hazards Methodology [80] outlines a comprehensive methodology for the assessment of combined external to IHs.

The methodology in the External Hazard Challenge Report [79] provides confidence in the ability of the design to withstand such EH/IH sequences. Safety measures that have been shown to be resilient to both EHs and IHs individually will, subject to a few exceptions described below, also be resilient to a consequential IH. This is because the IHs will also (frequently) require shutdown and, hence, initiation of safety measures to maintain the FSFs. The exceptions are:

- Infrequent IHs, as only safety category A functions are considered.
- IHs that are screened out because they do not result in failure of a duty system.

- Where redundancy is claimed by both the EH and IH assessments; and/or
- Where there is a cumulative effect, for example, EH loadings on a structure that is in a fire weakened state.

These exceptions will all be addressed as part of the more comprehensive assessment, however, confidence in the design's resilience to such events at DRP4 is argued based on the following:

- Although only safety measures supporting safety category A functions are assessed against infrequent IHs, the redundancy and segregation available in the safety measures supporting safety category B functions mean that there is a reasonable likelihood that the required function will similarly remain available.
- In the majority of instances, an IH sufficient to fail a safety measure will also have the potential to cause a failure of a duty system.
- The only design basis EH for which redundancy is claimed against the EH challenge (i.e. ignoring consequential IHs) is that of wind-blown debris affecting SSC located externally. The probability of failure of both trains, one due to a debris impact and the other due to a storm induced IH, is argued to be extremely low.
- Assuming seismic to be the most reasonably foreseeable cause of a consequential IH, and fire or flood to be the most likely IHs, these IHs would only be experienced after the seismic event. The target is for safety measures to be qualified against any of these hazards individually, i.e. full ongoing functionality (for example, no plastic deformation), thus ensuring that the characteristics that afford hazard resilience against the consequential IH are unaffected by the seismic EH.

The safety analysis of all EH/IH combinations will be undertaken as part of the site-specific assessment. However, the next update of this report will report the work undertaken to assess what is considered to be the dominant risk of seismically induced IHs.

3.3.3.4 Safety Assessment

The EH challenges identified in the External Hazard Challenge Definition Report [79] constitute the initiators for the PIEs in the Fault Schedule [6]. The deterministic claims remain that the safety measures necessary to support the CoR, CoFT, CoRM and CoRE FSFs will remain available during and post any credible combination of EHs.

The following sections describe each of the EH challenges along with the means of ensuring adequate resilience of the claimed safety measures. This resilience is achieved by either: requiring that the SSCs that constitute a safety measure are qualified against the unattenuated hazard challenge (i.e. full qualification), affording protection such that the SSCs do not experience the hazard challenge or somewhere between the two (i.e. affording hazard attenuation and qualifying the SSCs against the residual hazard challenge).

Any SSC to attenuate/remove the hazard challenges are classified according to the function they are protecting. Therefore, the protection/attenuation systems themselves are resilient to all EH challenges, including even those that they are not designed to address. This ensures that the design is resilient to all combinations of EHs that may reasonably be expected to occur simultaneously. It also ensures that EH resilience for consecutive hazards is captured.

There may be instances where affording full EH resilience to a protection/attenuation measure is deemed to be impracticable, for example, qualifying SSC that form part of the lightning protection measures against a design basis seismic event. Providing the EHs can be shown to be independent, then such non-conformities shall be permitted subject to an adequate ALARP justification.

3.3.4 Seismic Hazard

3.3.4.1 Introduction

Design basis and operating basis Peak Ground Acceleration (PGA) values for the seismic hazard are provided in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73]. It is acknowledged that seismic hazards are highly site-specific, however, ground motion has been generalised for the purpose of generic design development. Other primary and secondary seismic hazards such as liquefaction will be considered at the site-specific stage and, where necessary, mitigated by suitable modifications/mitigations (for example, soil improvement).

A series of ground models with differing strength and stiffness ranges are considered to represent a credible range of site conditions for which a RR SMR is likely to be deployed. The range of ground models is developed with reference to existing GB nuclear power station sites and geology [81]. The GB site (ground) type can range from 'soft' to 'very hard', which impacts the selection of the spectra value, shape profile and response. Bounding conditions have been assumed for the generic design.

Design Input Spectra (DIS) [82] are defined using the EUR standard shape response spectra, which will be used in future soil structure interaction sensitivity studies. The DIS is also used to develop Secondary Response Spectra (SRS) for the design of SSCs. Using a SRS for design rather than the DIS gives a more accurate gauge of the actual seismic demand placed on SSCs at their respective locations. SRS consider the resonance of the structure, damping and, in the case of SSC located within the Reactor Island, the effect of the SIS. The SRS are generated for six different locations on the SIS. The final SRS for each specified location will envelop the peak-broadened best estimate, lower bound and upper bound soil cases for all ground models. Further detail is presented in the SRS Technical Note [83].

The verification of SSCs to their representative SRS is discussed in the relevant Tier 1 systems engineering chapters 4 to 11.

3.3.4.2 Seismic Challenge

3.3.4.2.1 Hazard

This EH challenge [79] considers the following EHs:

- Seismic hazard (design basis accelerations, differential displacements and induced sloshing).

Independent meteorological EHs are assumed to be present during the occurrence of this EH challenge. Therefore, the following hazards are assessed at a severity equivalent to the event with a 1-year return period.

- Either high or low dry bulb air temperature.
- Rain (hydrostatic pluvial flood loading).
- Hail/snow/ice loading.
- Wind loading.

The first of the above hazards has the potential to affect material strength/resilience to fatigue failure and, hence, is to be allowed for in the design. The remaining hazards all have the potential to increase the structural loadings experienced during the seismic event and, hence, require incorporation into the performance modelling to ensure that the required withstand is achieved.

3.3.4.2.2 Hazard Protection

3.3.4.2.2.1 Seismic Classification and Qualification

The overall requirement for seismic protection is that SSCs that provide, support or protect (including the provision of hazard attenuation) part of a safety function shall be qualified against the seismic hazard at a magnitude dependent on the categorisation of the safety function they provide. There is, in addition, a requirement that severe accident safety functions, designated as Category C, withstand the design basis seismic event.

All SSC supporting a category A or B safety function, including those classified lower than the system they support on account of the grace time to their required operation, and those affording a severe accident function are to be qualified against the SRS applicable to the design basis seismic event for their location. This assessment considers all relevant failure mechanisms caused by either the accelerations or displacements (for example, resulting in contact forces with adjacent SSC) experienced during a seismic event.

Additional assessment is provided for those SSC relating to safety category A functions to demonstrate the absence of any cliff edge effects, i.e. that their function is maintained following a marginally more severe hazard challenge. Qualification is also provided where required to demonstrate that no other SSC can prevent the functionality of any of the above SSC.

Seismic classifications are defined in accordance with the methodology in Section 3.2 to provide clarity on the objective to be achieved, for example, whether a pump is required to operate during a seismic event or whether it is merely required to maintain an intact pressure circuit boundary. This ensures that the necessary safety function is available during and post a seismic event whist avoiding unnecessary design, etc. effort on maintaining non-safety significant functions.

Safety class 3 structures are precluded from impeding the functions of safety class 1 or 2 structures [84] by classifying them as SPC2. SPC2 structures are permitted to undergo plastic deformation and exhibit damage during and following a DBE, but such damage/deformation shall not result in interaction with a safety class 1 or 2 structure.

SPC1 or SPC2 structures are designed in accordance with the Civil and Structural Codes and Standards Policy [57]. Structures which are SPC3, or which do not have any seismic performance are designed in accordance with the Eurocodes.

3.3.4.2.2.2 Aseismic Bearing

The RR SMR design makes use of a SIS to attenuate horizontal displacements in a seismic event. This does not remove the requirement for seismic qualification of the SSC located on the SIS but instead serves to reduce the horizontal accelerations such that design/qualification is less onerous.

One adverse impact of this design feature is increased relative displacements between elements located on and off the SIS. This requires design provision to be made for pipe, cabling, etc. runs that pass on/off the SIS to accommodate the increased differential movements. There is also a change in frequency associated with the seismic motion of SSC on the SIS, which has the potential to lead to excessive seismic motion of free-surface fluids. The design for sloshing shall consider various mitigation measures, including appropriate damping characteristics for the SIS, design features to prevent overtopping of fluids, or demonstration that loss of water inventory does not have significant safety consequences.

Further detail on the SIS is provided in E3S Case Tier 1, Chapter 9B: Civil Engineering Works and Structures [44].

3.3.5 Meteorological Events

3.3.5.1 Introduction

Meteorological conditions (for example, wind, snow) also introduce loadings to SSC that are not afforded weather protection (for example, an enclosure). Two different bounding scenarios have been identified: one that addresses 'normal' storm conditions, whilst the other considers a tornadic storm. Characterised parameters for the associated meteorological conditions are summarised in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73].

3.3.5.2 Storm Challenge

3.3.5.2.1 Hazard

This EH challenge considers the following EH loadings on SSCs:

- Wind.
- Wind-driven missiles (impact loadings).
- Rain (hydrostatic pluvial flood pressure).
- Hail/snow/ice.

These EHs are all considered to derive from a common source and, hence, occur simultaneously at their design basis magnitude. These loadings are assumed to occur at extreme temperatures, i.e. either design basis high or low dry bulb air temperature [79].

The notable difference between the storm and seismic challenges is that full hazard resilience, as opposed to hazard reduction, can be achieved by affording a suitable enclosure that protects the SSC therein. This effectively passes the burden of hazard resilience onto the associated enclosure, along with an equivalent functional categorisation.

The overall requirement for protection against the storm challenge is that SSCs providing, supporting or protecting part of a safety function that are exposed to the associated loadings shall be qualified. As with the seismic challenge, all SSC supporting a safety category A or B Safety Function, including those classified lower than the system they support on account of the grace time to their required operation, as well as any severe accident measures, are to be (or afforded protection that is) qualified against the storm challenge.

Only SSC supporting safety category B functions need be considered, however, as those supporting safety category A functions are addressed by consideration of the Tornadic Storm challenge, see Section 3.3.5.3. As with all EH challenges, qualification that no other SSC whose failure under storm conditions could prevent a safety category B function shall be provided.

3.3.5.2.2 Hazard Protection

3.3.5.2.2.1 Hazard Shield

The Hazard Shield is a massive reinforced concrete structure that protects a significant proportion of the SSC delivering safety category A and B functions. It provides protection against all storm loadings for SSCs contained within. The Hazard Shield is designed to withstand an accidental or malicious aircraft impact, which bounds the loadings experienced during the storm challenge. Discussion of structural elements, interfaces and performance evaluation of the Hazard Shield are described in E3S Case Tier 1, Chapter 9B: Civil Engineering Works and Structures [44].

3.3.5.2.2.2 Systems External to Hazard Shield

SSCs located outside the Hazard Shield that are required to function during and after storm-related challenges are protected against in the following ways:

- Wind, rain and hail/snow/ice loadings: either qualification against the combined loading or the provision of a suitably qualified enclosure.
- Wind-driven missiles: the provision of redundant trains such that safety measure functionality is only lost in the (considered to be) highly unlikely event that wind-driven missiles damage both trains.

Examples are the Back-Up Generation System and the ESWS. Both systems are to be qualified to the design basis storm loadings and have redundant trains located to the north and south of Reactor Island, thus affording additional resilience to wind-driven missiles. The reasonable practicability of the provision of debris impact protection to these SSC shall only be pursued if the failure probabilities of the two trains are such that they are considered to be within the design basis, i.e. the overall frequency of an event leading to the failure of both redundant trains is >1E-4pa for SSC supporting safety measures affording a safety category B function and >1E-7pa for SSC supporting safety measures affording a safety category A function. Early work indicates that these target frequencies are likely to be supportable, but that work is still under consideration. Further discussion regarding the modelling of such events is described in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

Requirements for these systems can be found in E3S Case Tier 1, Chapter 8: Electrical Power [42] and E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43] respectively.

3.3.5.3 Tornadic Storm Challenge

3.3.5.3.1 Hazard

Tornadic storm has been identified as a separate bounding scenario to 'normal' storm, as the associated wind loadings are more onerous than that of a 'normal' storm for events less frequent than 1E-3 per year [29]. As this is only the case for infrequent events, only SSC supporting safety category A functions require consideration against this hazard challenge, including the cliff edge assessment of events marginally more severe.

The overall requirement for Tornadic Storm protection is essentially the same as for the 'normal' storm event, but with elevated wind speeds and associated wind-driven missile impacts [79], in addition to the requirement to consider cliff edge effects.

3.3.5.3.2 Hazard Protection

Hazard protection is analogous to that provided for the 'normal' storm event, noting that the design has preferentially located the SSC supporting the safety category A functions within the Hazard Shield where practicable. The notable supporting systems that are external to the Hazard Shield include: endurance water supplies, electrical generating capability (the LV DGs to float the batteries affording the safety category A supply function should both the grid supply and both of the HV Standby DGs fail) and elements of the HVAC systems.

None of these systems are required within the first 24 hours of a fault transient, however, they are necessary to achieve site autonomy for the mission time of 168 hours. They are all dual-train, redundant systems that are well separated.

3.3.5.4 Extreme Temperature/Humidity/Pressure Challenge

3.3.5.4.1 Hazard

This EH challenge considers other potential fault scenarios associated with extreme climatic conditions. These may be broken into performance challenges, for example, the ability to reject sufficient heat to the environment to maintain SSC within their defined temperature limits, and alternative failure mechanisms, such as the freezing of vent panel seals preventing their opening.

The parameters considered are:

- High or Low Dry Bulb or High Wet Bulb Air Temperature.
- High or Low Air Pressure.
- Icing (common with low air temperature only).

These EHs are considered to occur concurrently at their design basis magnitude [79].

3.3.5.4.2 Hazard Protection

For SSCs located within Reactor Island, the HVAC systems constitute the primary protection measure to maintain acceptable internal temperature and humidity ranges in the event of extreme external meteorological conditions. These systems may be considered as being in two parts: external Air Handling Units (AHUs) and the Reactor Island Chilled Water (RICW) system. The AHUs compensate for fluctuations in external ambient conditions by heating/cooling and humidity conditioning, as required, the incoming air supply. These are dual train redundant systems located either side of the reactor building that are designed to accommodate the maximum/minimum design basis parameters.

The RICW system affords a duty means of heat removal from individual areas where heat is generated using Local Cooling Units. It also supplies the Endurance Cooling tanks, which support the safety category A safety functions (for example, cooling of the DPS) in the event of chiller failure. As above, the chillers are designed to meet their performance requirements under extreme temperatures/humidities.

The Reactor Island HVAC systems are summarised in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43].

SSCs located outside of the Reactor Island that support safety category A and B functions are similarly designed to meet their required performance levels during extreme temperature/humidity events. For example, local air conditioning units will be supplied, as necessary, to ensure that the standby HV DGs and their supporting systems are maintained within their qualified temperature limits. Similarly, the ESWS cooling towers have been sized to accommodate the design basis extreme climatic conditions.

Protection against system failures, e.g. extreme low temperatures leading to freezing of water services, is addressed by: trace heating, insulation, HVAC systems and/or operating procedures (for example, a requirement for a system to be run during cold weather to maintain flow and hence temperature).

3.3.5.5 Lightning Challenge

3.3.5.5.1 Hazard

Lightning presents a unique challenge, as it has the potential to cause the failure of all electrical and C&I systems. Furthermore, the likely extent of such failures, i.e. the unmitigated fault sequence,

cannot be determined, as it is a function of multiple variables (the location of the strike, its magnitude, the SSC that afford a potential conduction pathway to ground, etc.). Thus, no arguments are made regarding the separation of redundant safety systems, but instead prevention of any failures to SSC supporting safety category A or B functions is sought.

The adverse consequences of this EH challenge [79] relate to lightning current effects, including sparking and EMI. The methodology for addressing EMI is described in the Electromagnetic Interference Methodology and Identification report [85] and is discussed further in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

The lightning event is assumed to occur during either design basis high or low dry bulb air temperatures and rain or drought. This ensures that any protection systems, for example, earthing, meet their design requirement during all EH events.

3.3.5.5.2 Hazard Protection

The Earthing and Lightning Protection System (LPS) comprises four sub-systems:

- Earthing/Grounding System [XFA].
- Equipotential Bonding System [XFB].
- External Lightning [XFC].
- Internal Lightning Protection [XFD].

These serve to address the three key systems for lightning protection: air termination, down conductor and earth termination. These are passive systems and, hence, the provision of a single high integrity engineered system achieves the deterministic targets.

In reality, however, other structures will also afford DiD protection. For example, the shell roof is the most likely air termination point for a significant proportion of lightning strikes to the site. As this is a steel structure, it is likely that it will also afford the down conduction pathway. It is unlikely to be claimed as formal protection, however, as substantiating the structure to all EH challenges (for example, Tornadic Storm) is deemed to be impracticable. Instead, systems forming part of/connected to the Reactor Island structures are likely to form the principal claim.

Assurance that the lightning currents do not constitute a potential EMI hazard to C&I systems is achieved by ensuring separations between the associated cabling and potential down conductors exceed the minimum defined safe distance. In instances where this cannot practicably be achieved, shielding (either as part of the cabling itself or to cabling conduits) is employed.

The final element of the lightning protection is the provision of surge protection. As this constitutes an active measure, the practicability of affording diverse, redundant systems to protect those electrical and C&I systems supporting safety category A or B safety functions will be determined through detailed design.

Further information regarding lightning protection is provided in E3S Case Tier 1, Chapter 8: Electrical Power [42].

3.3.6 Hydrological Hazards

Water ingress can also lead to system failures. This can be due to rainfall coming into contact with vulnerable SSC either directly or as a result of a leak path/ flooding. The latter can be further divided into: pluvial flooding (surface water accumulation due to precipitation), fluvial flooding (originating from rivers) and coastal flooding. Coastal and fluvial flooding are highly site-specific and cannot, therefore, be characterised for the purposes of assessing the generic design. Only pluvial flooding

has therefore been considered. Parameters are summarised in E3S Case Tier 1, Chapter 2: Generic Site Characteristics [73].

3.3.6.1 Flooding Challenge

3.3.6.1.1 Hazard

Even pluvial flooding is largely dependent on the location of the site, as surface water levels are not only a function of the porosity of the available drainage areas, but also the local topography with respect to the ability for any surface water to disburse or, in the worst case, accumulate in instances where areas of the surrounding land drain towards the site.

Suitable operating basis and design basis pluvial flood depths are to be defined. This will make no claims on the conventional site and plant drainage systems due to the high probability of blockage during a flooding event.

3.3.6.1.2 Hazard Protection

Where it is not practicable to qualify the relevant SSCs to the level of hazard corresponding to its location (for example, full submersion for components below the pluvial flood depth or in locations liable to the accumulation of rainwater), hazard protection is afforded.

For the majority of components requiring design basis hazard protection, this is afforded by the Hazard Shield. This will not only prevent rainwater impingement to SSCs contained within, but will also prevent any water ingress, thereby addressing the hazard of pluvial flooding. This requires that all penetrations are either located such that water ingress is effectively precluded (for example, unprotected external penetrations being located above the pluvial flood height) or afforded suitable watertight seals to preclude significant water ingress (for example, glanding to any services entering the structure).

It is recognised that this may be challenging in the case of accessways into the building, where entry/exit may reasonably be expected to be required during the period of the flood. Potential design solutions include their location above the pluvial flood depth and an inner barrier, containing the flood to a localised area. Where entry/exit can be precluded during the course of the flooding excursion, the additional option of affording an (essentially) watertight door is also available.

The above solutions recognise that the prevention of all water ingress is likely to be impracticable. Hence, a small ingress flowrate will be permitted. This shall be directed to suitable drainage sumps with sufficient capacity as to not make any claims on the systems employed for their emptying.

Similar concepts are employed to SSC located outside the Hazard Shield. These will either be qualified to the DBCs or be housed within a structure that keeps the necessary components dry. The function provided by any such structures will be assigned a categorisation equal to that of the function they are protecting. They will, therefore, also be required to demonstrate resilience to all other design basis external challenges; exceptions only permitted where an EH challenge is independent, e.g. seismic, and arguments can be presented that it is not reasonably practicable to qualify the structure to that external challenge.

It is noted that a number of the components external to the Reactor Building are located on plinths. These will afford a level of additional defence-in-depth, raising the relative height of the components mounted on top. An example of this is the Back-Up Generation Structure (BUGS) on which the Standby AC supplies are mounted [86].

3.3.7 Aircraft Crash

3.3.7.1 Introduction

An AAC into one of the structures, including the site berm, could lead to significant system disruption over a significant area of the site. Details on characterised aircraft can be found in the Aircraft Impact Hazard Definition Report [87]. The AAC rate onto the critical areas of the RR SMR site is estimated to be an order of magnitude below the design basis screening criteria at 1E-6 per year [87] [73].

3.3.7.2 Accidental Aircraft Crash Challenge

As a beyond design basis event, the provision of multiple safety measures is not deemed reasonably practicable. Instead, the safety measures affording the category A safety functions are sought, from a best estimate perspective, to achieve a level of hazard reduction to reduce the resultant risk to ALARP.

AAC [79] considers the following EH challenges to the relevant SSCs:

- Impact Loading.
- Impact Induced Shock.
- Aircraft Fuel Fire.

Only AAC is considered, as malicious aircraft crash forms part of the security considerations. Further detail on the methodology for addressing AAC is provided in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.3.7.2.1 Hazard Protection

3.3.7.2.1.1 Within Hazard Shield

Continued availability of the safety measures supporting the category A safety functions following AAC is principally maintained through the Hazard Shield. This is designed to withstand an AAC and protect equipment located inside from the consequential effects.

Impact-induced vibrations, as per seismic events, cannot be fully attenuated by the Hazard Shield, i.e. shock loads will be transmitted to the SSCs within. Vibration analysis is carried out to produce a bounding shock spectrum for this event [88]. The relevant safety measures are assessed on a best estimate basis against this resultant SRS.

3.3.7.2.1.2 Outside the Hazard Shield

Those SSC located external to the Hazard Shield that support category A safety functions are predominantly limited to systems that are only required to support the function either 24 or 72 hours after the event. For example, electrical supplies are supplied from batteries located within the Hazard Shield. It has been assessed to be impracticable, however, for these batteries to meet the full 7-day mission time. Hence, the LV Essential AC Generation System [BL], which is located external to the Hazard Shield, is provided to float the batteries to ensure that the required electrical load to support category A safety functions can last for the 7-day mission time.

These systems are (as a minimum) dual redundant trains that are typically located either side of the Reactor Building. Although this affords a significant degree of protection against the loss of both trains, it is judged the potential remains for an AAC that would result in the subsequent debris field affecting both trains. However, the nature of an AAC would not preclude the early provision of off-site support, as it would only affect an area local to the site; this is in contrast to fault sequences

initiated by natural EHs that could reasonably be expected to have a widespread effect on the surrounding infrastructure.

The exceptions to the above are a number of penetrations in the Reactor Building, for example, the Local Ultimate Heat Sink outlets to atmosphere. As these are located on opposing aspects of the Reactor Building, it is argued that from a best estimate perspective simultaneous failure of all redundant trains is highly unlikely.

3.3.8 Other Hazards

3.3.8.1 Introduction

The remaining three EHs relevant to the generic site are: LOOP, LOOW and solar-induced effects, termed Space Weather. The first two represent man-made EHs, albeit with a high likelihood of being consequential to natural EHs.

Characterised LOOP and LOOW durations and frequencies are described in the Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies Report [29]. A description of the Space Weather EH can be found in the Space Weather Hazard Methodology [89].

3.3.8.2 Loss Of Off-site Power Challenge

3.3.8.2.1 Hazard

This EH challenge considers a loss of electrical power to the site. The LOOP challenge is identified as being consequential to all other EHs, in addition to posing an EH in their absence. It covers both a failure of supply and the potential for degraded supply. The latter covers instances where voltage, frequency and/or waveform exceed the ranges specified in the Grid Code [90], thus leading to the potential failure of electrical and C&I systems. Further information around LOOP events is available in the Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies Report [29].

The frequency of a loss of supply for longer than 168 hours is assumed to be greater than (more frequent than) 1E-3 per year. Hence, the overall design basis target for LOOP protection is for two autonomous systems, both capable of meeting the 168-hour mission time. The first has a category B safety function for adequate onsite power provision to support the most onerous combination of safety measures supporting category A or B safety functions. The second system has a category A safety function to support only the safety measures supporting category A safety functions.

There is also a requirement for suitable protection measures to be available to ensure that a degraded supply is detected and isolated prior to causing any damage to the electrical and C&I systems. The aspiration is for two independent and, as far as reasonably practicable, diverse systems that will afford protection to the systems supplying the SSCs supporting the category A and B safety functions.

3.3.8.2.2 Hazard Protection

The LOOP protection systems are provided by two separate technologies: DGs and batteries. In the first instance, both systems rely on the batteries (the Essential Uninterruptible Power Supply Systems [BM_, BP_ and BQ_] [91]). Immediately following the LOOP, the batteries provide a supply to the applicable SSCs that use electrically powered equipment to respond to plant faults, as defined in the Fault Schedule [6]. The batteries [BMV and BQV] can provide power for a minimum of 24 hours.

On loss of grid supply, the two redundant DGs that form part of the HV essential AC Standby Supply system [BD] will be automatically started [92]. If at least one of these two starts, it automatically refloats all of the battery systems via the LV Essential AC Standby Supply system [BK], thus maintaining continuity of supply at all category A and B safety functions with an autonomous capability.

Should both of the HV DGs fail to start, either automatically or following operator intervention, then the LV Essential AC Standby Supply system [BL] can be manually demanded [92]. These are configured to support the category A safety functions.

Additional temporary external power connections are also provided for additional DiD to both the HV and LV systems to enable supply via local portable generators.

Protection against degraded grid supplies is also protected against by two separate systems. Each system is similarly aligned with either the HV or LV Essential AC Standby Supply systems. These systems are thus redundant and as diverse as practicable.

The electrical systems that protect against LOOP are summarised in E3S Case Tier 1, Chapter 8: Electrical Power [42].

3.3.8.3 Loss Of Off-site Water Challenge

3.3.8.3.1 Hazard

The LOOW challenge is equivalent to that of LOOP, noting there is no degraded supply hazard. For the purposes of the generic design, insufficient flow is bounded by no flow. In addition, the frequency of a LOOW for a given duration will be site-specific. It is assumed, however, that a LOOW event lasting for 168 hours or longer is a frequent event. The primary difference between LOOW and LOOP events is a difference in protection philosophy.

3.3.8.3.2 Hazard Protection

Instead of affording two water supply capabilities, the design approach is to provide dedicated reserve supplies for each system requiring an off-site water supply. This is analogous to the fuel supplies for the DGs used to supply the LOOP protection systems.

For a minimum of the first 24 hours of the hazard transient, the necessary water reserve is achieved by sizing the system's local water capacity such that it can perform its safety function without the requirement for water addition from a source elsewhere on site. For example:

- Protection against LOOW to the PDHR [JN02] for a minimum of 24 hours is provided by the design volume of the LUHS [JNK] tanks, which have been designed so only 2 out of 3 tanks are needed to supply the appropriate amount of cooling for 72 hours, without the need for top up.
- Beyond the 24-hour period, there is provision for the transfer of water supplies held onsite. Thus, the LUHS [JNK] tank(s) will be topped up either via the transfer of water between redundant LUHS [JNK] tanks or through the Safety Measure Coolant Supply [KAX] system [93] that takes water from ESWS tanks.
- Following 168 hours it is assumed that off-site resources will have been made available to provide a top-up water supply to the LUHS [JNK] tanks.

The other significant water demand supporting category A and B safety functions is to the ESWS [PB]. The redundant, dual-train cooling water towers have recirculation sumps that are topped up

with water to compensate for evaporative losses. Each train has its own local water supply that is capable of meeting the full 7-day autonomous mission time.

There is also DiD provided through the option to use water from the Fire Water Systems [XGB].

The LUHS [JNK] is summarised in E3S Case Tier 1, Chapter 6: Engineered Safety Features [39]. The ESWS and the Fire Water Systems [XGB] are summarised in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43].

3.3.8.4 Space Weather Challenge

Space Weather is a term used to cover the hazard posed by solar activity and its potential consequences on the RR SMR and/or its supporting services. The impact of this solar activity can be varied and widespread, including:

- Damage to electronic systems caused by solar energetic particle events.
- Loss of radiocommunications due to EMI caused by solar radio bursts.
- Adverse effects on the grid supply due to electromagnetic pulses generated by solar flares or geomagnetically induced current generated by coronal mass ejections.

There is a lack of historical data and OPEX for this EH, therefore work is ongoing to better understand the frequency and the severity of such events. At DRP4, the effects are considered to be bounded by other external (for example, LOOP) and internal (for example, internally induced EMI) hazard challenges.

3.4 Protection against Internal Hazards

3.4.1 Introduction

IHs are events arising from within the site boundary of the power station and are PIEs that could challenge the delivery of the FSFs. Most of these events originate inside buildings housing this equipment. However, events originating in other buildings, or outside buildings, within the site boundary, are also considered as IHs. IHs are introduced as a result of the systems and components required for the safe operation of the RR SMR and so they can be managed through good design.

This section provides a list of IHs (both individual hazards and combinations of hazards) considered in the design of the RR SMR, as well as supporting information to demonstrate that the SSCs supporting FSFs are adequately protected against the effects of IHs.

3.4.2 Principles of Internal Hazard Protection

The requirement for IH protection is to ensure:

- The FSFs continue to be delivered following IH design basis events and combination of hazards.

The demonstration that the design achieves protection against IHs is through ensuring the following safety requirements are maintained following a hazard:

- At least one set of redundant/diverse train of safety systems.
- Structural integrity of VHR equipment.
- The functionality of the MCR (if functionality is compromised the secondary control room must remain operable).

Generally, this is achieved through, segregation between redundant/diverse trains of safety systems, ensuring only one train of a safety system may fail by an IH event.

Where segregation is not provided between safety trains, then only one train of a safety system may fail by an IH event. In this case, either local protection, or by ensuring the safety system trains can withstand the hazard loads (or a combination of both) is demonstrated. Where SSCs have a withstand requirement these shall have the capability of withstanding the loads imposed by IHs (or combination of hazards). VHR equipment is protected from IHs, ensuring that they are not impacted, as far as reasonably practicable, otherwise ensuring that they can withstand the hazard loads that could be imposed upon them.

3.4.3 Approach to Internal Hazard Protection

3.4.3.1 Introduction

The Internal Hazards Strategy [94] contains the high-level strategy for undertaking of IH assessment for the RR SMR. The objective of the IH topic area is to identify the IHs that have the potential to affect nuclear safety, characterise these IHs and to provide input to engineering and design teams to ensure that the design of the RR SMR is protected from the impacts of IHs.

The approach to the assessment of IHs includes the following:

1. The identification of individual IHs, including combination of hazards.

2. The characterisation of IHs (severity, frequency, etc.).
3. Safety assessment on impact of IHs on the RR SMR
4. Application of IH requirements to design and layout
5. Verification that the protection measures meet the IH requirements.

The assessment of IHs (steps 1 to 3) and input to design (step 4) are iterative through the design process to reduce risks to ALARP. From early in the design iteration, IHs requirements from RGP have been allocated to SSCs and the layout to ensure that the challenge from IHs is minimised. Layout reviews [95] have been conducted to ensure the layout is optimised to eliminate or minimise the impact of IHs. These reviews have enabled optimisation of the layout with respect to IHs.

This stage of the process is iterative, and as the detailed design develops, the scope and depth of the reviews increase relative to the level of design detail available. At DRP4 the focus of the IHs has been ensuring that the layout is adequately segregated.

3.4.3.2 Hazard Identification

Hazard identification for IHs is primarily achieved via Area Datasheets, which are updated against the design using the RR SMR requirements database. The format of the Area Datasheets is such that all the required parameters are provided for every equipment item, making it possible to search the Area Datasheets for the purpose of hazard identification.

The Area Datasheets is a module within the requirements database which is populated by using the Functional Bill of Materials (FBOM) module and the Locations Register module. The FBOM presents a list of operating equipment that forms part of a system along with the various design parameters associated with each item of operating equipment, e.g. pressure and temperature. The Locations Register module stores the layout information for each item of operating equipment e.g. the Reactor Island Block, Train etc.

The Area Datasheets are supplemented by additional sources of information which supports the hazard identification process:

- Layout Reviews which confirm the location of key equipment in each area, including consideration of which of these could be IH sources.
- Design documentation (for example, SDDs, drawings, Piping and Instrumentation Diagrams), which provide additional information on equipment configuration/operation that may not be in the Area Datasheets.
- 3D model, which enables location of equipment to be identified more precisely than in the Area Datasheets.
- Engagement with block owners and system owners, who provide insight into the latest design developments prior to full integration into the design documentation.

Hazard Identification and screening for individual and combinations of all key hazards has been undertaken for each plant area, and a group of hazards has been identified for a particular area and a bounding hazard case defined and assessed (considering multiple / consequential hazards where applicable).

3.4.3.3 Analysis of Internal Hazards

The hazards identified in the relevant areas of the RR SMR have been analysed by applying the Internal Hazards Methodology [96]. This involves detailed analysis (where maturity is available) on the sources of IHs within the relevant layout areas.

The result of this analysis is reported in the summary reports:

- Internal Hazards Analysis Report: Electrical and C&I Systems Block [97].
- Internal Hazard Analysis report: Auxiliary and Waste Blocks [98].
- Internal Hazard Analysis report: Fuelling Block [99].
- Internal Hazards Internal Flooding Analysis Report [100].
- Internal Hazards Additional Fire Analysis Report – Impact on Civil Structures [101].
- Internal Hazards Local Fire Analysis Report [102].
- Internal Hazards within hazard shield analysis report [103].
- Internal Hazards Analysis - Outside Hazard Shield [104].

The results of early analysis are also used indicatively by the design teams for specific system studies. For example, indicative blast loadings were provided to the design teams of the accumulators to support a study into the potential resizing of the component.

IHs analysis results are further discussed in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.3.4 Safety Assessment

The internal hazards analysis has been used to inform deterministic safety analysis, discussed in Section 5 of the Internal Hazards Methodology [96]. The steps below show how deterministic safety analysis is applied to IHs:

1. Identify required safety measures.
2. Define Hazard PIE.
3. Characterise hazard and define effects on safety measures (unmitigated consequences).
4. Identify hazard protection.
5. Classify hazard protection and define performance requirements.
6. Record and substantiate hazard protection.

The required safety measures are based on the duty systems required in Modes 1 and 2 at DRP4 and will be extended to mode 6 as the design matures. The duty systems include:

- Systems in the block that are in operating mode 1 and 2, including any structure supporting the systems.
- VHR and HR equipment.
- Radioactive sources.

The IHs PIEs are listed in Section 3.14 (Appendix A) based on the Definition of PIEs and Derivation of Initiating Event Frequencies Report [29]. The report defines the PIEs and highlights the applicable operating modes and the IEF of the PIEs. The identified PIEs have been fed into the Fault Schedule [6] to identify where a hazard could cause a fault.

Based on the hazard analysis performed and engineering judgment, the impact of a hazard on the safety measure is assessed. Hazard protection measures and the various performance requirements are identified. Hazard protection measures are prioritised using the hierarchy of controls, (eliminate, reduce, isolate, control) preferring passive measures (barriers) over any active measures.

Hazard schedules and requirements tables [105] are produced to capture the findings and feed into the PIEs and Fault Schedule which captures safety categorised functional requirements on SSCs to ensure tolerance to IHs.

3.4.3.5 Verification and Validation

Evidence of verification for specific systems is provided in the corresponding Tier 1 systems engineering chapter for the system it is applicable to. For example, evidence of verification of Civil Engineering Works and Structures is found in E3S Case Tier 1 Chapter 9B: Civil Engineering Works and Structures [44].

Following the safety assessment process outlined in Section 3.4.3, the IHs analysis is then subject to V&V. This process follows the V&V approach described in Section 3.1.13, and is informed by the Approach to Design Verification for Internal Hazards [106]; the methods used for the analysis of the individual IHs are validated using this approach. The document details the methods of analysis, physical and simulated. The document also details the verification approach for the different IHs explored in the report, including the functional verification and transverse verification aspects for each hazard. The verification evidence will be captured in the RR SMR requirements management database.

Following verification, a design review is carried out to confirm that the layout iteration is tolerant to IHs.

3.4.3.6 List of Internal Hazards

The following individual IHs have been considered in the design of the RR SMR based on reviews of the site plan and RGP [94]:

- Internal Fires.
- Explosion.
- Flooding.
- Pipe whip.
- Missiles.
- Blast.
- EMI.
- Dropped Loads.
- Hazardous Materials.
- Vehicular Transport Accident (VTA).

For each of these individual hazards, subsequent sub-sections provide an overview of the safety requirements, main protection measures (preventive and protective), and the hazard analysis methods. E3S Case Tier 1, Chapter 15: Safety Analysis [5] summarises the results of the analyses described within each sub-section.

3.4.3.7 Combinations of hazards

In addition to hazards occurring as single events, some event sequences or equipment failures can lead to situations where SSC are challenged by multiple or “combined” hazards. Hazards combinations are categorised into three groups:

- Consequential Hazards: combinations where the primary hazard initiates a secondary hazard i.e. the cause of the secondary hazard is the primary hazard.
- Correlated Hazards: combinations of hazards where more than one type of hazard is initiated by the same underlying cause.
- Independent Hazards: combinations where there is no causal relationship between the hazard initiators. These types of combinations will only be considered for assessment if the individual hazard frequencies sum to give an overall frequency of >1 x 10^{-7}/yr.

Hazard combinations can be correlated, consequential or both and, given the nature of combined hazards, it is theoretically possible that several hazards could be initiated in a 'sequence'. Consequential sequences are described for each 'primary' IE leading to a primary hazard, which causes a 'secondary' IE followed by a secondary hazard. An example is illustrated in Figure 3.4-1, where a pressurised pipe failure leads to multiple correlated hazards (flooding, pipe whip and steam release).

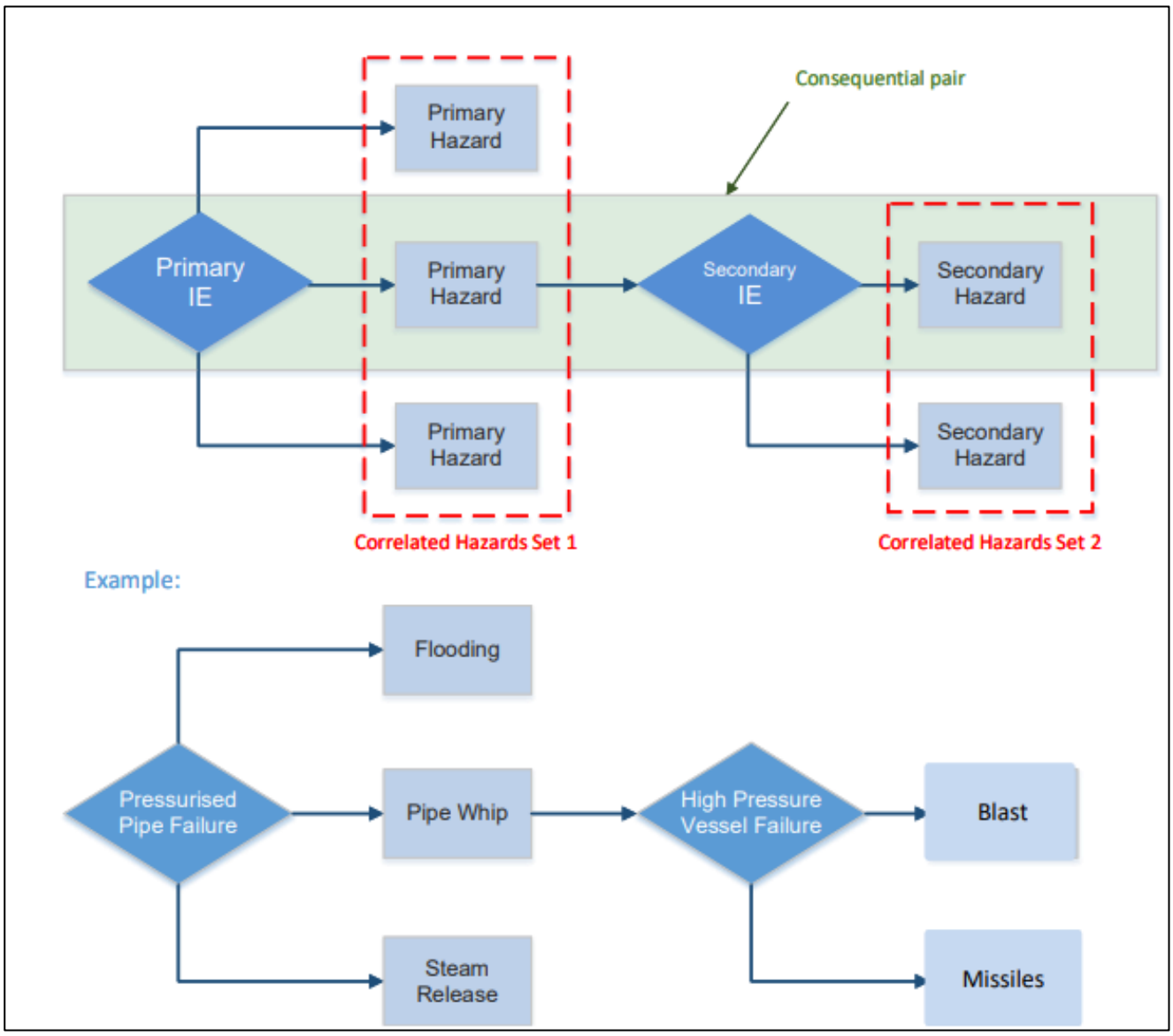


Figure 3.4-1: Internal Hazards Approach Flow Diagram

Tertiary events are not considered within a combined hazard sequence, as the frequency causing a significant hazard is considered outside of the design basis. Additionally, the approach to adding the worst-case loads corresponding to each credible sequence ensures that the assessment will remain conservative despite the omission of tertiary events.

The Internal Combined Hazards Methodology and Identification Report [107] details the approach to combined hazards and the method for identifying and screening combined hazards. The IH analysis reports (see Section 3.4.3.3) provide screening tables for each of the blocks in Reactor Island to identify the potential combinations of correlated hazards. The External-Internal Combined Hazards Methodology [80] approach to EHs causing IHs is discussed in 3.3.3.3.

Hazard screening ensures a proportionate response to analysis on hazard combinations, ensuring that only hazards combinations which could occur are analysed. Combinations of hazards which can occur on a hazard target are collated into combination tables to define the combined load that the hazard target must withstand as discussed in [107].

3.4.4 Internal Fires

3.4.4.1 Introduction

Internal fires are one of the major hazards on a nuclear power station due to the range of combustible materials as part of the SSCs, other plant, or miscellaneous items in storage. The design of the RR SMR considers fires to occur on site from:

- Building/solid material fires.
- Oil or other liquid pool fires.
- Gaseous fires.
- Oil mists.

The aspects covered for fire hazards are global effects and local effects for different types of fuel.

Global effects cover the assessment of a compartment fire and its effect on the barriers and structures globally. They are characterised by global fire parameters in the compartment such as compartment temperature evolution in time, smoke layer position and temperature, Heat Release Rate (HRR) and gas composition.

Local effects consider the effects of fire on targets such as structures and equipment that can be affected by direct flame impingement, radiation effects or plume impingement. Local effects are characterised mainly by flame length, plume temperature and incident radiation on a target.

Internal fire introduces additional hazards such as flooding (from fire suppression systems) which are considered as part of IHs.

3.4.4.2 Safety Requirement

The assessment of internal fire safety demonstrates that no single fire event, located anywhere on site, can lead to a set of plant conditions where FSFs (covering all aspects of the safety case) could be lost. The impact of internal fire on nuclear significant SSCs must ensure that:

- A fire does not impair the functionality of more than one set of redundant trains of safety systems.
- A fire does not impair the functionality of non-redundant SSCs which perform safety functions.

- A fire must not compromise the functionality of both main and supplementary control rooms.

3.4.4.3 Protection Measures

3.4.4.3.1 Overview

Fire protection measures are developed in accordance with:

- ONR - Internal Hazards TAG [108].
- IAEA – Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants [109].

Along with codes focused more on conventional safety:

- Fire Safety: Approved Document B (ADB) [110].
- BS 9999:2017 Fire Safety in the design, management and use of buildings – Code of Practice [111].

Fire protection measures focus on the elements required for the plant to fulfil nuclear safety requirements, however, are also balanced against the conventional and commercial aspects:

- Nuclear safety focuses on ensuring that a safe shutdown state can be achieved. This focuses on segregation of nuclear safety significant SSCs such that a single fire event cannot not impair the functionality of one than one set of redundant trains of safety systems or lead to a radioactive release.
- Conventional safety ensures that the provisions are included to ensure that personnel can escape to safety and allow access for the local authority fire brigade. This introduces escape distance requirements, protected fire escape routes, and firefighting provisions.
- Commercial aspects such as commercial and business continuity requirements look to include enhanced protections to prevent significant down time or reputational damage.

These combine to form the site fire strategy [112]. The design implements three types of fire protection measures:

- Reduction.
- Isolation.
- Control.

3.4.4.3.2 Reduction

The design has eliminated combustible materials and ignition sources, where reasonably practicable. For example, concrete and steel are used for the main civil structures and modules are non-combustible. Sources of ignition (hot surfaces, flames and hot gases, mechanically generated sparks, electrical apparatus, exothermic reactions (chemical), spontaneous ignition and static charge) are eliminated so far as is reasonably practicable.

Fire loads are reduced using fire-retardant materials such as low combustibility cable and reducing the quantity of stored combustible materials. Where combustible materials cannot be avoided, storage areas are identified, documented and segregated from ignition sources and safety related plant/equipment.

Systems which contain a flammable liquid or gas are designed with a high level of integrity. Protection measures such as bunds, drip trays/guards and flange shields control and contain any leakage of combustible or flammable liquids.

3.4.4.3.3 Isolation

If a fire were to occur, the main protection measure is through segregation to limit the spread of fire between redundant trains of SSCs. For nuclear significant SSCs and nuclear material, this is achieved through fire compartments which ensure that independent redundant SSCs are not impacted by a single fire event. Further fire compartmentation is included to satisfy lifesaving requirements of fire management. However, penetrations in divisional fire barriers (such as doors, dampers, cable and pipework penetrations) are avoided where practicable.

All of the SSCs which form the boundary of a fire compartment are designed to withstand the impacts of a fire. Barriers segregating redundant trains of safety systems are rated to 4-hour fire resistance to the standard fire curve (BS EN 1363) as an indicative design load until the modelling is completed. Fire dampers are provided in ventilation ducts that penetrate fire barriers to prevent the transmission of fire and smoke between divisions.

Where divisional segregation is not possible, spatial segregation is used to ensure that a fire cannot propagate but also prevent a fire from causing the failure of two redundant trains of SSC. This is achieved by ensuring that there is sufficient distance between the combustible material and all other redundant trains for damage to be avoided.

3.4.4.3.4 Controls

Whilst there is a preference for passive fire protection measures, fire detection and fire-fighting systems [XG] are provided to minimise the fire risk, with the necessary systems defined by conventional safety and loss prevention requirements. The systems are designed to provide a timely alarm in the event of fire, and/or its prompt extinguishing. These minimise the adverse effects on personnel and items important to safety but are not claimed for nuclear safety. Examples include fire detection and alarm systems, fire suppression systems, and fire and smoke dampers in vent ducts.

Fire detection systems, fire extinguishing systems and support systems such as ventilation and drainage systems should, as far as practicable, be independent of their counterparts in other fire compartments to maintain the operability of such systems in adjacent fire compartments. Fire suppression systems should not present further risks to class 1 and 2 systems. Water-based fire suppression systems should be provided with adequate drainage routes and components at risk of water damage should be protected against spray.

Fire protection measures are described in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43].

3.4.4.4 Hazard Analysis

3.4.4.4.1 Overview

Design verification for internal fire is through deterministic assessment of all on-site sources using area data sheets to identify hazard sources. Operators and equipment affected by the release are identified based on the release locations using area datasheets and operational documentation.

The main principles which are applied to the hazard analysis [96] are:

- Fire is assumed to occur in any room/area which contains combustible materials, (i.e. an ignition source is assumed to be always present).
- All combustible inventory in the room/area contributes to the fire load.
- Where a room contains at least one source of flammable liquid, the largest fuel load is considered to leak and create a liquid pool fire.

Internal fire is assessed for both global and local effects of a fire as required to demonstrate the design is robust to the hazard. Both analyses provide a hazard loading for the target SSCs that can be used ensure that the barriers perform as requirement against a fire, or if there is a need for addition protection measures.

Results of the analysis carried out for internal fires is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.4.4.2 Global Fire Analysis

The global fire analysis focuses on ensuring the integrity of the divisional segregation. Bounding case rooms are selected by considering fires that pose the most significant threat to the barriers or other SSCs important to safety. The bounding cases have been modelled to provide a hazard loading for the fire barriers. US National Institute of Science and Technology (NIST) fire modelling tool CFAST is used as the primary tool to perform fire modelling, this can be supplemented by Computational Fluid Dynamics (CFD) as required.

3.4.4.4.3 Local Fire Analysis

Local fire analysis focuses on ensuring that specific target SSCs can withstand the effects of a fire. Typically, these targets are Class 1 and 2 SSCs with are not segregated, VHR and HR components, SSCs requiring hazard protection to prevent or respond to hazard scenarios which are not bounded by the fault analysis. Fire and Targets SSCs are identified using the area data sheets. The modelling of the fire analysis primarily uses Fire Dynamic Tools (FDT), supplemented by CFD as required.

3.4.5 Internal Explosion

3.4.5.1 Introduction

An internal explosion is a violent expansion in which energy is transmitted outwards as a shock wave originating from within the site boundary. Explosions can lead to pressurisation of rooms as well as blast waves that can challenge divisional segregation, directly damage equipment important to nuclear safety and result in a radiological release. The potential sources of internal explosions are:

- Flammable gas explosions (explosions within buildings).
- High Energy Arcing Fault (HEAF).
- Vapour Cloud Explosion (VCE) (explosions external to buildings).
- Oil mist release.

The explosion is considered to occur during normal operation of the reactor (during power operation or during shutdown). However, assessments are also made against the most onerous plant conditions.

3.4.5.2 Safety Requirements

The assessment of internal explosion safety demonstrates that no explosions event, located anywhere on site, can lead to a set of plant conditions where FSFs could be lost. In addition to the general IH requirements outlined in 3.4.2, as explosions have the potential to initiate further consequential hazards, explosions should not affect the stability/integrity of safety classified buildings and fire safety barriers.

3.4.5.3 Protection Measures

3.4.5.3.1 Overview

Explosion protection measures are developed in accordance with:

- The Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR 2002) [113].
- BS EN 60079 - Explosive Atmospheres [114].

3.4.5.3.2 General Protection Measures

Explosion sources are eliminated by design through replacing flammable gases or vapours with non-flammable alternatives as far as reasonably practicable. Priority is then given to protection measures that limit or prevent the formation of explosive atmospheres. The impact of explosion is reduced through minimising the operating pressures and temperatures as well as stored volumes. Avoiding operating above the superheat limit temperature to avoid the effects of a Boiling Liquid Expanding Vapour Explosion (BLEVE). Fuel oil systems are not pressurised to reduce the risk of explosive atmospheres, as far as reasonably practicable.

Ignition sources are minimised where there is the potential for an explosive atmosphere. DSEAR 2002 zoning providing the correct ATEX rating for electrical equipment to minimise the ignition risk. Explosive atmosphere areas are categorised/zoned accordingly using appropriate methodologies (for example, DSEAR 2002 and BS EN 60079-10). Adequate risk assessments are required in areas where explosive substances are present during normal operation under the requirements of DSEAR 2002.

If an explosion were to occur, the main protection measure is through segregation to limit the spread of the explosion between redundant trains of SSCs. Due to the risk of explosions causing fires, the components which make up the boundary of fire compartments are designed to withstand the effects of an explosion.

3.4.5.3.3 Explosive Gases and Vapours

Explosive gases and vapours are stored in well-ventilated compounds away from SSCs and safety classified buildings. Preferable selection of storage cylinders of small volumes reduces the associated magnitude of an explosion from a single cylinder. Gas cylinders are segregated from each other based on proper classification of the gas (flammable, oxidiser, inert). Flammable gases, oxidizers and combustible materials are segregated from each other to avoid undesirable reactions.

Where explosive gases are required or produced inside of buildings, adequate ventilation is available to prevent the creation of an explosive atmosphere, in accordance with DSEAR 2002.

3.4.5.3.4 High Energy Arcing Fault

Physical explosion hazards, such as those created by HV electric arcing, are minimised by the appropriate selection of electrical components (for example, breakers) and by system design, to limit the probability, magnitude and duration of potential electric arcs. For HV switchgear and electrical panels, arc ducts safely vent arc flash pressure and hot gases from HV panels.

3.4.5.3.5 Oil Mist

Oil mist explosions may occur if oils are pressurised and so using unpressurised oil where possible is preferential. Flange guards to contain the spray from pressurised systems containing oil at the most likely leak points segregating oils mists from sources of ignition.

3.4.5.4 Hazard Analysis

Design verification for internal explosion is through deterministic assessment of all on-site sources using area data sheets to identify hazard sources. Operators and equipment affected by the explosion are identified based on the explosion locations using area datasheets and operational documentation.

Analysis on explosions depends on the type of explosion and the characteristics of the material causing the explosion. The methodologies [96] follow the same format:

- Identify the explosion source.
- Characterise the type of explosion (flammable gas, HEAF, oil mist, vapour cloud explosion).
- Determine the magnitude of the explosion.
- Calculate the explosion load on target SSCs.

The magnitude of the explosions determined using conservative assumptions such as (double ended guillotine breaks on pipework, arc time can be taken as 1 s for HEAF, stoichiometric oil mist explosions).

Explosion analysis is performed using the most appropriate tool for the explosion source (Multi-Energy-Method, impulse method, FLACS, PHAST, R3) as outlined in the Internal Hazard Methodology [115].

Results of the analysis carried out for internal explosions is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.6 Internal Flooding

3.4.6.1 Introduction

Internal floods are defined as floods arising within the site boundary, both inside and outside buildings. They are generated by postulated failures of equipment containing liquids such as tanks, pipes, pumps and valves either through factors such as valve misalignment, over-pressurisation, corrosion, material embrittlement/fatigue or caused by another hazard. Once generated, they have the potential to lead to loss of many SSCs if left unmitigated due to spray or submergence.

The systems and structures which are liable to fail during flooding are:

- Electrical and C&I equipment, except for cables whose terminals are not flooded and where the equipment is protected against water ingress.
- Certain civil structures that are not qualified to resist the floodwater pressure or its temperature.
- Non-watertight mechanical equipment.

External sources of flooding from natural events, including snow and rain are considered in the external flooding assessment.

3.4.6.2 Safety Requirements

The assessment of internal flooding safety demonstrates that no single flood event, located anywhere on site, can lead to a set of plant conditions where FSFs could be lost. In addition to the general IH requirements outlined in 3.8.1 the following safety requirements are applicable to internal flooding:

- A flood must not affect the stability/integrity of safety classified buildings and divisional barriers.
- No postulated flooding events shall result in loss of floodwater to the outside or otherwise to the environment.

3.4.6.3 Protection Measures

3.4.6.3.1 Overview

The design implements three types of flood protection measures:

- Prevention.
- Isolation.
- Control.

3.4.6.3.2 Prevention

Sources of flooding cannot be eliminated from the design of a power plant, but the size of equipment is optimised to its functional requirements, limiting the overall potential to create a flood. Stored quantities of liquid are kept to the minimum required for safe operation of the plant.

3.4.6.3.3 Isolation

The primary protection measure against internal flooding is through divisional segregation of redundant trains. For the purposes of internal fooding, a retention volume is defined. The retention volume is designed to contain all the volume of the most onerous flooding cases in each division. This is enabled by the design of the structure to allow for the downward passage of floodwater through drains and other flooding specific measures. The boundaries of a flooding retention volume includes watertight doors, openings and any other penetrations to avoid loss of floodwater to other retention volumes or the environment.

All equipment that is important to safety is located:

- Above the maximum expected transient flooding height from any postulated flooding event or alternatively designed to be robust to submersion.
- Away from any flooding initiator that may result in cascading water or condensation or alternatively designed to be robust to cascading water and condensation.
- Away from any flooding initiator that may result in spray or alternatively designed to be robust to spray.

3.4.6.3.4 Control

Where the flooding initiator is large and risks the divisional segregation integrity, additional measures are in place, namely isolation of the flooding source. Leak detection within the flooding source and/or drainage system informs the operators in the MCR as to a flooding event, allowing for isolation of the flooding source.

3.4.6.4 Hazard Analysis

Design verification for internal flooding is through deterministic assessment of all flooding sources within a flooding zone to ensure that divisional segregation is maintained. All flooding initiators are considered; however, only one of the initiators is postulated to occur at any one time, unless two or more initiators have a common identified cause (for example, multiple failures after earthquake) [96].

Flooding analysis requires identification of all flooding zones and flood retention volumes and the flooding sources within. The potential flow rate and volume of each flooding source within a flooding zone is calculated without any mitigations. Conservatively, it is assumed that the pipework undergoes double ended guillotine break and there is no mitigation of the flooding source. If the unmitigated flood is not tolerable, mitigations (isolation, flow restrictions) are claimed to calculate the mitigated flood volume.

Once the flood is characterized, the effect of the flood on all SSCs as it traverses the flooding zone through to the retention volume are calculated. This identifies the hydrostatic pressure exerted by the floodwater on divisional barriers and all SSCs that could be lost in a flood either through submergence or spray/condensation

Results of the analysis carried out for internal flooding is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.7 Pipe Whip

3.4.7.1 Introduction

When a pressurised pipeline is severed, the fluid escaping from the open end exerts a thrust on the pipe. This thrust results in the application of a bending moment to the pipe, which may exceed that necessary to cause the pipe material to be in a plastic state across the whole cross-section and therefore, a plastic hinge develops.

Where this occurs, the continuing thrust generates a rapidly accelerating rotational displacement of the section on the break side of the plastic zone. This phenomenon is called pipe-whip. Equipment within the zone swept by the whipping pipe, which is dictated by the extent of plastic deformation along the length of the pipe, may therefore be at risk and hence the potential damage to objects within the hazard zone must be assessed.

3.4.7.2 Safety Requirements

Failure of pressurised systems in the form of pipe whip could affect both the safety function of the failed system and the function of the target SSCs impacted by the event.

The safety requirements for a pipe whip demonstrates that no single event, located anywhere on site, can lead to a set of plant conditions where FSFs (covering all aspects of the safety case) could be lost.

3.4.7.3 Protection Measures

Elimination of the pipe whip is not reasonably practicable, but the likelihood can be significantly reduced through application of safety measures, notably for design, manufacturing, construction, and surveillance. Minimising the operating pressures and temperatures, stored volumes and overpressure devices limit the potential damage a pipe whip event can cause.

After application of good design practices, the main protection measure for pipe whip is through segregation of redundant SSCs, including:

- Divisional separations acting as barriers between redundant trains.
- Layout design placing safety class 1 and 2 SSCs out of reach of postulated pipe whip events.
- Local Barriers to protect SSCs.
- Pipe whip restraints, limiting the impact area for a pipe whip and reducing energy imparted to barrier.

3.4.7.4 Hazard Analysis

Design verification for pipe whip is through deterministic assessment of all pressurised pipework to identify the potential pipe whips and determine the bounding consequences. Effects such as jet impingement are considered to conservatively identify the bounding consequences [96].

The hinge location is assumed to occur at the wall. The hinge is likely to form closer to the failed end of the pipe than the wall. The length of the whipping pipe is chosen based on the maximum room/ area dimensions. It can therefore be assumed for initial assessments that the full length of the pipe can present a failure point, independent of locations of welds and pipe features.

The magnitude of the pipe whip and therefore the consequences are dependent on the characteristics of the pressurised pipework design, contents, operating conditions. The layout also drives the potential scale of the pipe whip.

Results of the analysis carried out for pipe whip is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.8 Internal Missiles

3.4.8.1 Introduction

Equipment failure can lead to the generation of internal missiles which then can be propelled for long distances and cause significant damage to nuclear significant SSCs. The main sources of internal missiles are:

- Failure of pressurised equipment.
- Failure of rotating equipment.

The potential sources of internal missiles depend on the component that fails as well as the material within.

3.4.8.2 Internal Missiles from Vessels

Missiles could be generated by failure of a pressurised vessel. The RR SMR design considers all vessels subject to pressure vessel burst as sources of internal missiles if they contain:

- Steam.
- Pressurised gas.
- Water above atmospheric pressure and a temperature above the superheat limit.

Fragmentation of pressurised components can lead to the generation of internal missiles with high velocities which can then be propelled for long distances and can cause significant damage. The impact of the missile on the target SSC depends upon the fragment size/mass, number, kinetic energy, initial velocity and range. The size and number of the fragments is partially dependent on the nature of the failures, i.e. if they are brittle or ductile.

3.4.8.3 Internal Missiles from Valves

Missiles could be generated by failures of valves on pressurised pipework. The design considers all valves as sources of internal missiles if they contain:

- Steam.
- Pressurised gas.

- Water above atmospheric pressure and 100 °C.

Valve bodies are usually constructed in such a manner that they are substantially stronger than the connected piping. Hence, it is generally accepted that the generation of missiles resulting from the failure of the valve body itself is sufficiently unlikely. The removable parts like valve stems or the valve bonnet, however, present a significant potential for failures that can lead to the production of missiles.

3.4.8.4 Internal Missiles from Rotating Equipment

Missiles could be generated by failures of rotating equipment such as pumps, fans, compressors, electric motors and turbines. Examples of rotating components whose disruptive failure may lead to the ejection of fragments as missiles include:

- Turbine generators.
- DGs.
- Gas compressors.
- Water pumps.
- Air fans.
- Electric motors.

Rotating components are generally enclosed by stators and/or casings or housings which may be able to contain the fragments. If the fragments can perforate the casings, an additional line of containment is often provided by the boundary of the plant area which contains the rotating plant item. Characterisation of missiles originating from rotating equipment is primarily based on impeller/rotor (or a disc in the case of a turbine) diameter and thickness, mass of the rotating part, and rotational frequency and speed. Generated missiles are of two basic types:

- Pieces, such as blades, that become detached from the rotating assembly.
- Segments of a rotating disc-like assembly that disintegrates, such as a flywheel.

3.4.8.5 Safety Requirement

Failure of rotating plant and pressurised systems could affect both the safety function of the failed system and the function of the target SSCs impacted by the missiles. The safety requirements for an internal missile demonstrates that no single missile event, located anywhere on site, can lead to a set of plant conditions where FSFs could be lost.

3.4.8.6 Protection Measures

The main preventive measure is to eliminate the potential sources of internal missiles, with the design using valves designed to prevent valve stems from becoming missiles and casings on rotating machinery designed to contain the loss of a rotor.

Where elimination is not reasonably practicable, the energy of internal missiles is reduced through:

- Minimising the operating pressures and temperatures.
- Minimising stored volumes.
- Addition of protection devices (for example, overpressure and over-speed protection for the steam turbine).

Barriers are included between divisions to ensure segregation of redundant trains and locally where internal missile sources and SSCs cannot be adequately segregated. Where the addition of barriers which can contain the impact of the internal missiles is not practical (for example, turbine failure, valve stem), the internal missile source is orientated to direct projectiles away from SSCs.

Routine inspection procedures and monitoring (for example, vibration) is implemented for significant internal missile sources such as high energy pumps to reduce the potential for failures to occur.

3.4.8.7 Hazard Analysis

Design verification for internal missiles is through deterministic assessment of all pressurised equipment to identify the potential missile sources and determine the bounding consequences [96].

The energy of any missiles produced by these sources can be calculated using R3 Impact Assessment Procedure or Center for Chemical Process Safety (CCPS) Document and compared with the capacity for any target SSCs or barriers claimed to protect the SSCs. Conservatively, the assumption of a hard impact is taken to maximise the energy which the barriers must withstand.

Results of the analysis carried out for internal explosions is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.9 Blast

3.4.9.1 Introduction

Failure of pressurised equipment (pipework and vessels) can lead to the creation of pressure waves referred to as blast. The strength and shape of a blast wave produced depends on many factors, including type of fluid released, the energy it can produce on expansion, rate of energy release, shape of vessel, type of rupture and surrounding characteristics.

The potential sources of blast are:

- All components containing water above atmospheric pressure and a temperature greater than the superheat limit.
- All components containing steam.
- All components containing gas above atmospheric pressure.

3.4.9.2 Safety Requirement

The safety requirements for a blast demonstrates that no single blast event, located anywhere on site, can lead to a set of plant conditions where FSFs (covering all aspects of the safety case) could be lost.

3.4.9.3 Protection Measures

The main preventive measure is to eliminate the potential sources of blast. Where this is not reasonably practicable, the impact of a blast is reduced though minimising the operating pressures and temperatures as well as stored volumes and avoiding operating above the superheat limit temperature to avoid the effects of a BLEVE.

If the hazard analysis demonstrates that that the risk of a blast is not minimised to a tolerable level, additional protection measures may be applied to the detailed design, such as use of blast walls to protect the SSCs important to safety.

3.4.9.4 Hazard Analysis

Design verification for blast is through deterministic assessment of all pressurised vessels to identify the potential blast sources and determine the bounding consequences. Effects such as ductile and brittle failure are considered to conservatively identify the bounding consequences [96].

The magnitude of the blast and therefore the consequences are dependent on the characteristics of the pressurised vessel design, contents, operating conditions. Depending on the type of blast, either the Guidelines for Vapor Cloud Explosion Pressure Vessel Burst, BLEVE, and Flash Fire Hazards [115] or R3 Impact Assessment Procedure 2009 are used to determine the energy associated with the blast.

The released energy associated with the specifics of the layout are then used to assign an overpressure and duration which is compared with the capacity for any SSCs or barriers claimed to protect the SSCs.

Results of the analysis carried out for internal explosions is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.10 Electromagnetic Interference

3.4.10.1 Introduction

The emission of electromagnetic radiation can cause disturbance which could affect the electrical circuitry, known as EMI. Such a disturbance may interrupt, obstruct or otherwise degrade or limit the effective performance of the circuit and hence associated function, or may result in unwanted spurious operations of a circuit. This could impact safety related functions of a nuclear site, resulting in failure of a critical system if not managed correctly.

Sources of internal EMI may be classified as:

- Natural and man-made sources.
- Intentional and unintentional sources.
- Fixed and portable sources.

3.4.10.2 Safety Requirements

EMI considers the impact on SSCs due to the interference from equipment which can generate an electromagnetic field and its impact of other plant equipment. The assessment of EMI covers Radio Frequency Interference (RFI).

The safety requirements for the hazard of EMI are to avoid loss of trains due to EMI shall be limited to a maximum of one train of electrical and C&I, safety fluids and back-up DG.

3.4.10.3 Protective Measures

EMI protection measures are developed in accordance with:

- BS EN 61000 Series [116] – Electromagnetic compatibility.
- BS EN IEC 62003 [117] – Nuclear power plants – Instrumentation, control and electrical power systems – Requirements for electromagnetic compatibility testing.

The impact of EMI as an IH is managed at source, by selecting equipment which limits the radiated and conducted EMI of all equipment.

The primary protection measure is through EQ. EQ, with regards to Electromagnetic Compatibility (EMC) can be split into two categories: requirements for electromagnetic emissions and requirements for electromagnetic immunity. EMC is achieved by limiting equipment emissions, requiring minimum equipment/system immunity levels and controlling electromagnetic coupling paths.

Divisional separation is introduced for redundant cables within C&I and electrical systems important to safety to ensure independence of systems performing a safety function, such that they can continue to operate regardless of the failure of any other system. Cables which are likely to interfere are located on separate cable trays (power cables and low-level electrical signals, cables of different voltage levels that form part of a safety class 1 system).

The simplest method of maximising EMC is the zoning of equipment within a given room and areas of the site by placing equipment with the highest potential for generation of EMI with similar equipment and locating it away from more sensitive equipment. The main approaches applied for zoning are:

- Creating zones of different degrees of interference potential (partitioning the system).
- Erecting barriers between the zones.
- Applying protection at the electrical interfaces across the barriers.
- Providing a dedicated reference earth which is segregated from the rest of the site. Note that at the time of writing this document it has not been determined that separate earthing systems will be required so the design does not currently include them.

Filters in the EMC context prevent interference from being imposed on equipment via conductive coupling but also helps to reduce radiated coupling if the interference is radiated to or from the cables that connect to the interfaces of the equipment. In addition to providing environmental protection, metallic enclosures also provide shielding from electromagnetic disturbances.

During the operational life of the plant, EMC performance of equipment, systems and components can change during service as a result of ageing, degradation or damage (e.g. to gaskets of enclosures, earthing connections, filters or surge protection). Regular inspections as part of routine maintenance procedures with regards to EMC will ensure continued correct installation and that any necessary corrective action is taken. Operational procedures are described in E3S Case Tier 1, Chapter 13: Conduct of Operations [12].

3.4.10.4 Hazard Analysis

Design verification for EMI is through deterministic assessment of all EMI sources within a room/area to ensure that consequences of EMI are tolerable. All sources of EMI are considered, especially non-classified equipment and portable equipment which may have less stringent EMC requirements [85].

EMI analysis requires identification of all sources of EMI. The boundary of each electronic system should be defined including its signal, power and earth ports. All equipment and systems performing fundamental or supporting safety functions, for each of the areas/rooms are identified. For all identified equipment and systems, an assessment shall be performed to determine the risk of interference and the likely consequence at both the equipment and system level based on Table B.1 of BS IEC 62003 [117]. Where an interface is identified, it is assessed by reviewing in detail the immunity characteristics of the receptor system. Equipment proposed for use should be qualified such that it meets the requirements of the appropriate EMC standards.

Results of the analysis carried out for EMI is summarised in Section 11 of the ‘EMI Methodology and Identification’ report [85].

3.4.11 Dropped Loads

3.4.11.1 Introduction

A dropped load is any item that is dropped or swung (pendulum effect where the load moves independently), or is a collapsing load (load exceeds weight limit therefore collapses for buckles). An impacting load is an object falling or colliding (vertically and laterally) with a component, or a structure.

Events considered within the scope of dropped loads are:

- Drop or swing of a lifted item: This occurs because of a lifting device failure causing loss of control of the load.
- Collision of a handled item: Uncontrolled horizontal movements of lifting and handling equipment which have the potential to cause damage to other SSCs.
- Falling Objects: Any item of plant which has not been lifted but which is located at an elevated level compared with other SSCs and which may become dislodged. Loose items such as equipment temporarily stored at height should be considered but also fixed items where it is feasible for these to become loose.
- Collapsed Structures: Failure of a structure causing it to collapse onto the SSCs it houses.

The risk of collapse of civil structures is deemed to be low, as structures are conservatively designed against hazards to a level commensurate with their consequence of failure. For example, buildings containing equipment required to operate after earthquake are seismically classified. Similarly, objects which are fixed in place are assumed to not fall provided they are seismically qualified.

3.4.11.2 Safety Requirements

Dropped loads considers the impact on SSCs due to the failure of lifting/mechanical handling equipment. Dropped loads could both impact nuclear significant SSCs as well as result in direct radioactive consequences (damage to fuel or waste packages). In addition to the general IH requirements outlined in 3.4.2, the following safety requirement is applicable to dropped loads:

- Nuclear inventory shall be protected against dropped loads.

3.4.11.3 Protective Measures

Lifting operations and equipment are developed in accordance with:

- Lifting Operations and Lifting Equipment Regulations 1998 (LOLER 1998) [118].
- LOLER 1998 Approved Code of Practice and guidance (ACoP) for Lifting Operations [119].
- Provision of Use of Work Equipment Regulations 1998 (PUWER 1998) [120].

Mechanical handling is required for the operation of the RR SMR and so cannot be eliminated from the design. The potential for dropped loads is minimised through optimisation of the number of lifting operations across the plant. The use of dedicated lift paths minimises interactions with nuclear significant SSCs.

Additionally, lifting devices are classified to align with the category of safety functions and classification of the SSCs affected by a potential dropped load event. Higher requirements placed on the lifting devices in association with procedures for lifting operations reduce the risk of an uncontrolled load.

Where the risk of a dropped load cannot be eliminated, the height of the lift is minimised, and barriers (reinforced walls and floors) are implemented where practicable to reduce the consequences of a dropped load. Structural supports are designed against collapse leading to drops onto SSCs.

Mechanical handling measures that provide preventive and protective functions for the fuel route are described in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43].

3.4.11.4 Hazard Analysis

Design verification for dropped loads is through deterministic assessment of all mechanical handling faults. The consequences of the dropped load are determined based on:

- Load that could be dropped.
- SSCs the load could impact.
- Energy imparted to the load and SSCs.

Dropped loads originating from mechanical handling faults are assessed, including but not limited to, fuel handling. Effects such as swinging and toppling of loads are considered as part of identifying the bounding consequences [96]. IHs assess all remaining potential dropped loads not covered by the mechanical handling assessment (e.g. falling objects), noting that these may be bounded by the mechanical handling assessment. Conservatively, the assumption of a hard impact is taken to maximise the energy which the SSCs or claimed barriers must withstand. The energy of the dropped load is compared with the capacity for any SSCs or barriers claimed to protect the SSCs.

Results of the analysis carried out for dropped loads is summarised in E3S Case Tier 1, Chapter 9A: Auxiliary Systems [43] and E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.12 Hazardous Materials

3.4.12.1 Introduction

Various hazardous materials that are located either permanently or temporarily on the site have the potential to be released. Such releases may occur due to failure of storage vessels, failure of pipework, or errors during delivery and transfer operations. Hazardous material releases have the potential to disperse either inside or outside of buildings and subsequently impact equipment or affect personnel carrying out actions important to safety.

This can occur mainly through the following effects:

- Toxic effects – could be harmful and/or fatal to personnel.
- Asphyxiation effects – could cause a reduction in the amount of oxygen available (due to release of Carbon Dioxide and Nitrogen) resulting in causing harm to the working personnel.
- Corrosion effects – could cause corrosion to SSCs and in turn threaten the performance of safety related plant.

Hazardous material release could result in other hazards (e.g. fire and explosion).

3.4.12.2 Safety Requirements

Hazardous material release could both impact nuclear significant SSCs as well as result in direct radioactive consequences. The main requirements for hazardous release are to ensure:

- The habitability of the MCR.

- Operators can perform necessary safety measures following a release.

The storage of hazardous materials on the RR SMR is in accordance with:

- Control of Major Accident Hazards Regulations 2015 (COMAH 2015) [121].

Assessment of the design against the COMAH 2015 regulations is outlined in E3S Case Tier 1, Chapter 31: Conventional Environmental Impact and Other Environmental Regulations [24].

3.4.12.3 Protection Measures

Management of hazardous materials follows the standard hierarchy of hazard controls. Therefore, hazardous materials have been eliminated from the RR SMR design where reasonably practicable. Where hazardous materials are required, the following measures are applied:

- Minimisation of the number of materials stored, preferentially storing in smaller containers to minimise the release from a single failure.
- Storage of hazardous materials away from where a release is likely to impact personnel (for example, away from the MCR).
- Appropriate ventilation to prevent the build-up of a hazardous material.
- Bunds and leak detection systems to contain toxic and corrosive leaks.

3.4.12.4 Hazard Analysis

Design verification for Hazardous Material release is through deterministic assessment of all on-site sources using area data sheets to identify release sources. Operators and equipment affected by the release are identified based on the release locations using area datasheets and operational documentation.

Dispersion modelling is applied [96] for the release scenarios using conservative assumptions:

- Catastrophic rupture and release of entire inventory of storage.
- Low wind speed to minimise dilution.
- Wind blowing in the worst-case direction.

Appropriate threshold concentrations of the toxic or asphyxiant gases are used to determine if the consequences are acceptable.

Results of the analysis carried out for hazardous material release is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.4.13 Vehicular Transport Accident

3.4.13.1 Introduction

Loss of control during the transport of materials and equipment in nuclear plant has the potential to trigger events with nuclear safety consequences. The hazard associated with movement of transport vehicles that may affect localised SSCs on site, either directly by impact, or consequentially arising from on-site hazardous sources or transported loads is termed a VTA.

The design basis events are divided into vehicles which may operate inside buildings (such as forklift trucks) and those which can only operate outside buildings (but inside the site boundary) such as delivery tankers. For UK nuclear sites, the external building speed limit is typically 10 to 15 mph, but consideration for vehicles exceeding this limit is given.

3.4.13.2 Safety Requirement

VTA could both impact nuclear significant SSCs as well as result in direct radioactive consequences. The safety requirements for a VTA demonstrates that no single VTA event, located anywhere on site, can lead to a set of plant conditions where FSFs could be lost.

3.4.13.3 Protection Measures

Elimination of onsite transport vehicles is not possible for the operation of the RR SMR, therefore SSCs are protected from the VTA hazard. This is achieved through the following measures:

- Rerouting vehicle transport routes and vehicles away from sensitive areas of plant as far as reasonably practicable.
- Controlling the speed of vehicles to reduce the severity of impacts through engineering means where practicable (for example, road bends).
- Installing appropriately designed energy absorbing barriers (such as walls, post or bollards).

3.4.13.4 Hazard Analysis

Design verification for VTA is through deterministic assessment of all potential on-site vehicles on the RR SMR site to ensure that they cannot adversely impact SSCs important for safety.

The assessment of the nuclear safety risk of VTA [96] from vehicular transport on site considers internal impact for a vehicle authorised to enter a safety classified building, or outdoor impact of a vehicle impact for a vehicle travelling on a road next to a safety classified building.

A set of target SSCs are identified based on where vehicles can impact. Safety targets more than 10 metres from the route or road are excluded in line with Eurocode 1.

The energy of the bounding VTA is compared with the capacity for any SSCs or barriers claimed to protect the SSCs. These events conservatively assume:

- Vehicles moving at their top speed.
- Targets are hard.

Results of the analysis carried out for VTA is summarised in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

3.5 General Design Aspects for Civil Engineering Works of Safety Classified Buildings and Civil Engineering Structures

The RR SMR civil engineering works and structures are designed in accordance with the general design requirements described in Section 3.1.7. E3S Case Tier 1, Chapter 9B: Civil Engineering Works and Structures [44] provides further detail on the design approaches and design basis for civil engineering works and structures, including foundations and the SIS. It also summarises the verification activities and seismic qualification in accordance with the EQ approach described in Section 3.9.

3.6 General Design Aspects for Mechanical Systems and Components

The RR SMR mechanical systems and components are designed in accordance with the general design requirements described in Section 3.1.7. Details of the design basis for mechanical systems and components are presented in:

- E3S Case Tier 1, Chapter 5: Reactor Coolant System and Associated Systems [40].
- E3S Case Tier 1, Chapter 6: Engineered Safety Features [39].
- E3S Case Tier 1, Chapter 9A: Auxiliary Systems [47].
- E3S Case Tier 1, Chapter 10: Steam and Power Conversion Systems [45].
- E3S Case Tier 1, Chapter 11: Management of Radioactive Waste [17].

The specific design aspects related to substantiation of the structural integrity of safety-classified pressure boundary components and their supports is summarised in E3S Case Tier 1, Chapter 23: Structural Integrity [4].

3.7 General Design Aspects for Instrumentation and Control Systems and Components

The RR SMR C&I architecture and systems are designed in accordance with the general design requirements described in Section 3.1.7. E3S Case Tier 1, Chapter 7: Instrumentation & Control [41] provides further detail on the general design approaches and design basis for the overall C&I architecture to ensure appropriate DiD, and the design basis for each safety classified C&I system.

3.8 General Design Aspects for Electrical Systems and Components

The RR SMR electrical architecture and systems are designed in accordance with the general design requirements described in Section 3.1.7. E3S Case Tier 1, Chapter 8: Electrical Power [42] provides further detail on the general design approaches, design rules and design basis for the overall electrical systems architecture to ensure appropriate DiD, and the design basis for each safety classified electrical system.

3.9 Equipment Qualification

3.9.1 Equipment Qualification Approach

EQ is defined by the IAEA as "the generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements".

The RR SMR approach to establishing EQ is through the Approach to V&V [67] to substantiate SSCs, rather than by a separate process, and includes environmental qualification and seismic qualification.

The definition and conducting of EQ activities ensure that SSCs will perform their allocated safety function(s) in all normal, faulted, and accident conditions for the duration of their operational lives.

The EQ approach includes three main steps:

- Define – the design inputs required to establish EQ.
- Establish – conduct verification that the equipment meets its design requirements, under required service conditions.
- Preserve – control and maintenance of the EQ through plant life.

An EQ framework is established [122] for the 'Define' step to guide the compiling of design inputs and requirements to support EQ activities, which include:

- Design requirements:
    - E3S functional requirements.
    - Non-functional performance requirements, including:
        - How well the function must be performed.
        - Mission times.
        - Target design life and EMIT activities.
- Service conditions for normal, abnormal and accident conditions (according to the plant state that the SSC is claimed), including:
    - Environmental conditions (external to equipment), including bounding mild conditions during normal operation and bounding harsh conditions following a PIE or hazard combination.
    - Operating conditions (internal to equipment/process driven), including normal bounding conditions and fault or accident bounding conditions following a PIE or hazard combination.
    - Seismic conditions.
- List of equipment requiring EQ.
- Equipment safety classification and seismic classification.
- Identification of codes and standards.

The methods used to 'Establish' and conduct EQ follow the same rationale for verification of the design definition described in Section 3.1.13, but also considers codes and standards specific to EQ.

For example, American Society of Mechanical Engineers (ASME) QME-1 code may be used for active mechanical equipment.

EQ design inputs are captured as SSC requirements within the Tier 2 Requirements Specifications. The EQ methods and activities for an SSC are documented in the Tier 2 verification strategy. Evidence of EQ outputs will be provided in the Tier 2 verification compliance reports, which will also capture any EMIT changes required for the 'Preserve' step of EQ. EQ evidence is summarised within the Tier 1 systems engineering chapters 4 to 11 of the E3S Case.

3.9.2 Seismic Qualification

Seismic qualification is achieved through an overall seismic design and verification approach adopted for RR SMR [123]. Seismic verification is applicable to all SSCs important to safety, which are required to be designed to withstand the effects of earthquakes (i.e. those assigned an SPC), whilst still being able to meet their safety categorised functional requirements, including both structural integrity and any active functions.

The seismic design approach ensures the SSCs can cope with the effects of the hazards generated during a seismic event, in accordance with the specified performance criteria and in compliance with the identified safety requirements. Seismic qualification is part of the process of seismic design, summarised below and in Figure 3.9-1.

- Define global inputs, including:
    - Define site/boundary conditions, including ground models to be considered.
    - Establish overall site layout and geometry.
    - Establish the DIS for defined damping levels.
    - Establish the safety classification and SPC.
    - Establish the global seismic analysis methodology.
    - Establish seismic analysis and design approaches for different types of SSC.
- For each SSC:
    - Establish the seismic hazard safety categorised functional requirements, safety classification and SPC for the SSC.
    - Formulate the SSC attributes including geometry, layout, structural form, material specification, loading etc.
    - Define the applicable codes and standards.
    - Establish seismic motion of and then demand on the SSC either directly via Quasi-Static methods, Response Spectrum Analysis or through SRS or Time History (TH) data.
    - Carry out seismic verification of the SSC, to show the design meets its requirements.
    - Produce the SSC substantiation evidence and output any requirements such as EMIT, relevant to Through-Life Activities (TLAs).
    - Provide any outputs necessary for downstream SSC qualification.
    - Carry out the necessary TLAs to maintain seismic qualification, including maintenance and monitoring, etc.

Verification methods align to more general verification methods outlined in Section 3.1.13, specifically including:

- Finite Element (FE) analysis or hand calculations in accordance with the relevant codes and standards.
- Rig Tests:
    - Code Verification: required to directly verify code requirements are satisfied. for example, novel elements of design.
    - Exploratory, proof, fragility tests.
- Similarity, where a candidate SSC is contextually similar to a type already qualified.
- Earthquake experience, analogous to similarity above, employing the use of experience data.

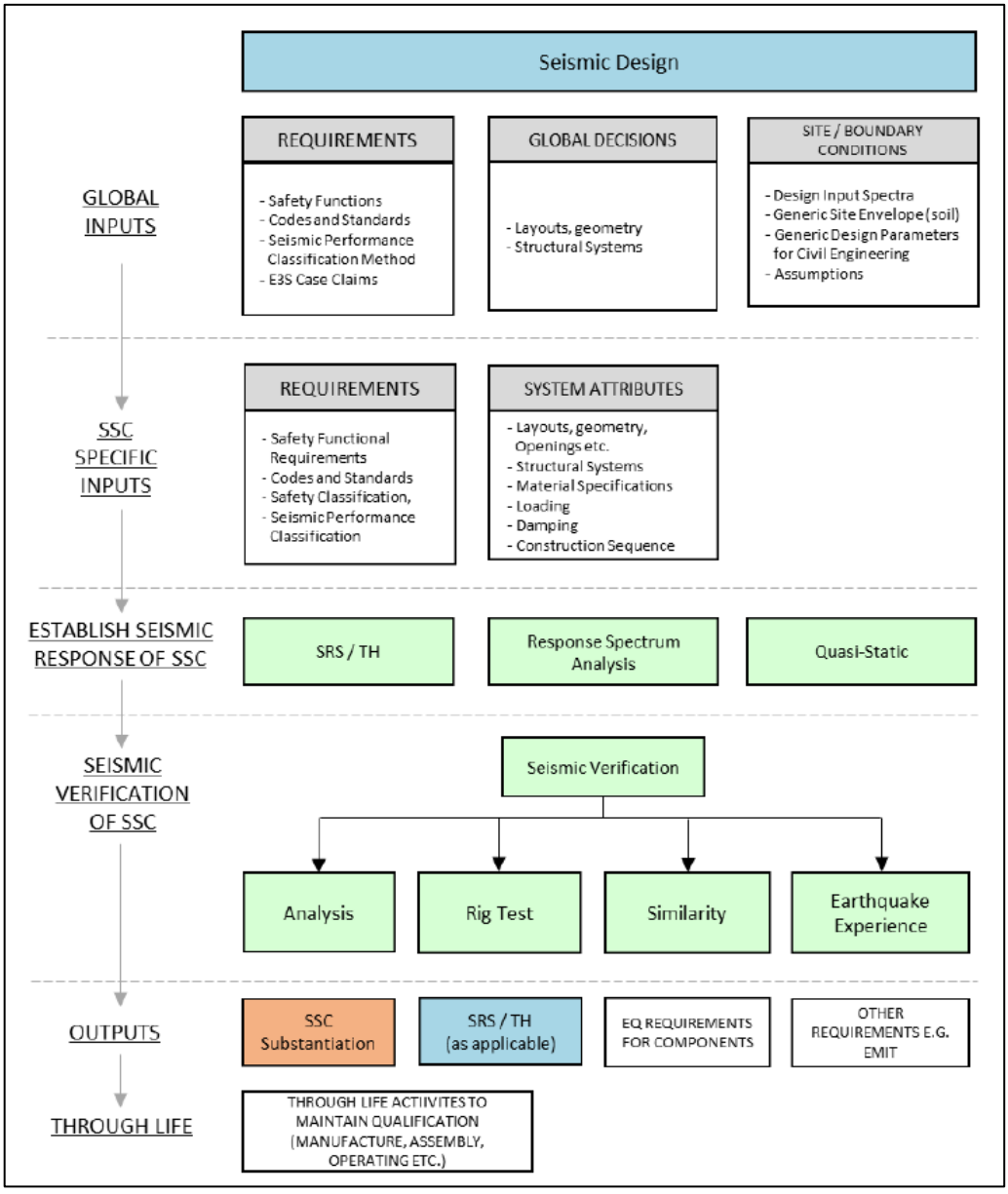


Figure 3.9-1: Seismic Design Summary

The seismic qualification activities for an SSC are documented in the Tier 2 verification strategies. Evidence of seismic qualification will be provided in the Tier 2 verification compliance report, which will also capture any EMIT changes required for the preservation of seismic qualification.

3.10 In-Service Monitoring, Tests, Maintenance and Inspections

3.10.1 Design Bases and Requirements

EMIT is an integral part of the operation of the RR SMR in support of equipment reliability for safety, environmental protection, legal compliance, and plant availability. EMIT ensures that the levels of reliability and availability of all E3S classified SSCs remain in accordance with the assumptions and intent of the design, underpinning claims that SSCs can deliver their E3S requirements through-life.

The RR SMR plant and SSCs are required to facilitate EMIT through definition of TLAs and provision of adequate space requirements in the layout, as described in the general design requirements for E3S in Section 3.1.7. The design is also required to ensure appropriate ageing management through effective EMIT strategies, described in Section 3.1.12.

A fundamental approach has been established for the design of SSCs and their associated EMIT activities [124]. This covers the development of EMIT tasks in accordance with RGP and OPEX, such as The EUR Association and EPRI utility requirements.

Types of EMIT tasks include:

- Surveillance tests or inspections performed to confirm availability/operability of an SSC in line with the E3S Case requirements.
- Preventive maintenance activities to prevent a failure or monitor degradation, including planned, predictive, or periodic.
- Corrective maintenance activities in response to a failure.
- Deficient maintenance activities in response to a potential or actual deficiency that does not affect SSC performance.

A graded approach to application of EMIT is adopted according to the functional importance of the SSC. For example, predictive and preventive maintenance activities may be employed on functionally critical equipment such as safety classified SSCs, whereas restorative maintenance activities may be applied to equipment with the lowest functional importance.

The graded approach to application of EMIT includes assessment of the level of risk associated with failure of an SSC. It considers the balance between the benefits of EMIT to increase reliability, with the competing negative effects on availability and the potential to introduce maintenance driven faults into SSCs, and the potential hazards to the operator(s) performing the EMIT activities, including potential dose.

Design for EMIT is documented in the Tier 2 SDDs/SMDDs for each SSC and summarised across the Tier 1 systems engineering chapters of the E3S Case. As EMIT activities are developed through the design process, they are stored within the RR SMR requirements management database with appropriate traceability to the design and the E3S Case. This will include traceability to technical specifications and OLCs (covered in E3S Case Tier 1, Chapter 16: Operational Limits and Conditions [13]).

3.10.2 In-Service Monitoring

Performance monitoring covers a wide range of activities to sense, record, analyse and assess the condition of SSCs. The design of SSCs facilitate the performance monitoring and data collection

through provision of appropriate instrumentation. Data will be used in future operational programmes to analyse and assess SSC condition and performance, operational effectiveness, and efficiency and effectiveness of EMIT strategies. Operational programmes are described in E3S Case Tier 1, Chapter 13: Conduct of Operations [12].

3.10.3 In-Service Testing

Inspection and test requirements that inform the design of SSCs primarily originate from design codes and standards (Section 3.1.7.6). This enables In-Service Testing (IST) and In-Service Inspections (ISI) through the life of the RR SMR plant to comply with the requirements defined in laws, regulations, codes and standards, including (but not limited to):

- ASME Section III (Material, Design, Fabrication, Examination, Testing).
- ASME Section V (Non-Destructive Examination).
- ASME Section IX (Welding).
- ASME Section XI (In-Service Inspection).
- ASME QME-1 (Qualification for Active Mechanical Equipment).
- BS EN IEC 62271 - HV Switchgear and Switchgear.
- IEC 60034-Series (Motor, Generator).
- IEC 60076-Series (Transformer).
- IEC 60896-Series (Battery).
- IEC/IEEE 60780-323 (Electrical equipment of the safety system - Qualification).
- IEC 60980 (Seismic qualification of electrical equipment of safety system).

The ASME Operation and Maintenance of Nuclear Power Plants (O&M) code sets specific design rules for IST on active components (pumps, valves). These design rules are described further in E3S Case Tier 1, Chapter 23: Structural Integrity [4].

3.10.4 In-Service Maintenance

The design of SSCs and layout to enable EMIT will facilitate preventive and corrective maintenance programmes for SSCs to be defined, using a graded approach in accordance with the EMIT strategy [124]. Operational programmes are described in E3S Case Tier 1, Chapter 13: Conduct of Operations [12].

3.10.5 In-Service Inspection

Inspection requirements for SSC are defined using design codes and standards, described in Section 3.10.3. Components and supports that use the ASME BPVC Section III design and construction code are designed to specific rules for ISI to detect defects which may propagate to a critical size. The rules set the scope of ISI EMIT (for passive pressure retaining parts) in accordance with ASME BPVC XI Division 1. These design rules are described further in E3S Case Tier 1, Chapter 23: Structural Integrity [4].

3.11Compliance with National and International Standards

An extensive and thorough review of national and international regulations and standards for nuclear facilities has been undertaken to develop the suite of E3S design principles [1] for RR SMR. Compliance with these E3S design principles supports achievement of the overall E3S fundamental objective 'to protect people and the environment from harm'.

The CAE framework [3] adopted for the E3S Case [2] presents high-level claims for the Tier 1 chapters that are derived from the E3S design principles. Arguments and evidence presented to underpin these claims ultimately provides the structured demonstration that the RR SMR complies with, or provides confidence that the design is capable of complying with, the E3S design principles to ultimately achieve the E3S fundamental objective.

The introduction section of each Tier 1 chapter provides a narrative of the key claims pertinent to that chapter, with reference to the relevant sections that pull together and summarise the arguments and evidence with reference to underpinning Tier 2 and 3 documentation. It also lists the interfacing chapters where relevant claims are covered. As the E3S Case is developing through the lifecycle, the conclusions of each chapter briefly summarise the further information still to be developed to underpin claims for that chapter.

Furthermore, relevant topic-specific regulations, codes and standards are listed within the introduction section of each chapter. The design and/or analysis information presented within that chapter summarises the compliance evidence against them.

3.12 Conclusions

3.12.1 Conclusions and Forward Look

This chapter presents the arguments and evidence for how the E3S design principles are applied to the design approaches and analysis of the RR SMR and achieve the claims in Section 3.0.3. Fundamentally, the E3S design principles are derived and justified based on an extensive set of UK and international RGP, which provides confidence that the framework for ongoing design and evaluation of RR SMR is suitable and justified.

The process for systematically identifying PIEs and sentencing for safety analysis is based on sound hazard identification methods and is complemented by use of RGP for existing PWRs. Hazard identification studies will continue alongside the developing design to feed into the evolving Fault Schedule and analysis, however, at this stage the list of PIEs is representative and comprehensive to inform the bounding safety analysis presented in E3S Case Tier 1, Chapter 15: Safety Analysis [5].

The fundamental functions for safety, environment and security are developed, and measures are assigned to deliver them, including safety measures across the DiD. Significant DiD is identified through measures providing safety functions related to the reactor and waste systems, and the fuel route. The safety measures for fuel route are in an earlier stage of design maturity, however, the allocation of safety functions at this stage ensures they are being designed to deliver their assigned functions and reduce risks to ALARP, demonstrate BAT, and ensure security and safeguards by design, in accordance with integrated E3S and engineering processes. Further opportunities for safety measures to enhance DiD to reduce risks to ALARP will be explored as the deterministic and probabilistic analysis continues through detailed design.

Functions for safeguards are not yet allocated to SSC; however, the plant layout and relevant SSC are being designed in accordance with safeguards requirements to ensure their design facilitates the delivery of specific safeguards functions, which will be allocated at the site-specific stage.

Functions are categorised and SSCs are classified in accordance with methodologies that are developed using industry best practices. Methodologies are applied for safety classified SSCs and KEPE that comprise environmental measures. Security functions are allocated to the PPS and CPS, and SSC that contribute to delivery of the functions are identified and classified. Requirements to enable safeguards functions are implemented in the design and layout.

Protection of safety classified SSCs against all credible EHs and IHs is achieved through separation and segregation and provision of safety measures to ensure FSFs are maintained. Safety measures are identified for all hazards, noting further opportunities to reduce risks to ALARP will be explored as the hazards analysis continues through detailed design. Site-specific hazards will be characterised and addressed in a future site-specific E3S Case.

The design principles, requirements and codes and standards for the plant layout and measures are presented, with more stringent requirements placed on higher safety classified measures. These requirements are developed based on RGP and are implemented through the integrated E3S and engineering processes. Their application to layout, measures, and SSC is described in the Tier 1 systems engineering chapters 4 to 11.

The general design approaches for radiation protection, conventional safety, ageing management, EQ, and EMIT are presented. The approaches are developed in accordance with RGP, and their application to the design is presented within relevant chapters of the case.

The generic E3S Case objective at Version 3 is ‘to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it’s developed through detailed design’.

The information presented in this chapter demonstrates that the E3S design principles are adopted in the approaches for design and analysis to achieve this objective. The iterative nature of the analysis will lead to further refinement of functions and measures in future revisions of the E3S Case to support the demonstration of ALARP, BAT, and secure/safeguards by design. However, E3S analyses have informed the design from outset, which provide confidence that the design is capable of delivering the E3S fundamental objective. Evidence of application of the approaches to the achieve the Version 3 objective is presented throughout the relevant chapters of the E3S Case.

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

None identified for this chapter at this revision.

3.13 References

[1] Rolls-Royce SMR Limited, SMR0001603, Issue 2, “Environmental, Safety, Security and Safeguarding 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, SMR0004363, Issue 4, “Environment, Safety, Security and Safeguards Case, Version 3, Tier 1 Chapter 23: Structural Integrity,” August 2025.

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

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

[7] Rolls-Royce SMR Limited, SMR0004487 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 24: ALARP Summary,” August 2025.

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

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

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

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

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

[13] Rolls-Royce SMR Limited, SMR0004555 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 16: Operational Limits and Conditions,” August 2025.

[14] 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.

[15] Rolls-Royce SMR Limited, SMR0004599 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 21: Decommissioning and End of Life Aspects,” August 2025.

[16] Rolls-Royce SMR Limited, SMR0004682 Issue 4, “Environment, Saftey, Security and Safeguards Case Version 3, Tier 1, Chapter 32: Generic Security Report,” August 2025.

[17] Rolls-Royce SMR Limited, SMR0004502 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 11: Management of Radioactive Wastes,” August 2025.

[18] Rolls-Royce SMR Limited, SMR0010327 Issue 1, “E3S Case Version 3, Tier 1, Chapter 25: Minimisation of Radioactivity,” August 2025.

[19] Rolls-Royce SMR Limited, SMR0010322 Issue 1, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 26: Sustainability,” August 2025.

[20] Rolls-Royce SMR Limited, SMR0008113 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 27: Demonstration of Best Available Techniques," August 2025.

[21] Rolls-Royce SMR Limited, SMR0010323 Issue 3, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 28: Sampling and Monitoring Arrangements," August 2025.

[22] Rolls-Royce SMR Limited, SMR0004486 Issue 4, "E3S Case Version 3, Tier 1, Chapter 29: Quantification of Radioactive Waste Disposals," August 2025.

[23] Rolls-Royce Limited, SMR0004490 Issue 4, "E3S Case Version 3, Tier 1, Chapter 30 Prospective Radiological Assessment," August 2025.

[24] Rolls-Royce SMR Limited, SMR0004514 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 31: Conventional Environmental Impact and Other Environmental Regulations," August 2025.

[25] The National Archives, "Health and Safety at Work etc. Act 1974 c.37," The National Archives, London, United Kingdom, 1974.

[26] European Council Directive, "89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work," Official Joural of the European Communities, Luxembourg, 1989.

[27] Rolls-Royce SMR Limited, SMR-STD-050 Issue 1, "Hazard Identification and Production of the Fault Schedule Standard," April 2024.

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

[29] Rolls-Royce SMR Limited, SMR0001389 Issue 5, "Rolls-Royce SMR Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies," February 2025.

[30] Rolls-Royce SMR Limited, SMR0004916 Issue 3, "FS (Fault Schedule), SM (Safety Measures) and Plant States DOORS Module Extracts," February 2025.

[31] Rolls-Royce SMR Limited, SMR0000510 Issue 3, "Rolls-Royce SMR C&I Engineering Schedule," August 2024.

[32] Rolls-Royce SMR Limited, SMR0023654 Issue 1, "Risks Assumptions Issues Dependencies Opportunities Log," May 2025.

[33] Rolls-Royce SMR Limited, SMR0005655 Issue 2, "Rolls-Royce SMR: Functional Security Categorisation and Classification Methodology," September 2023.

[34] Rolls-Royce SMR Limited, SMR0009908 Issue 2, "Rolls-Royce SMR: Integrated Security Solution," March 2025.

[35] Rolls-Royce SMR Limited, SMR0000636 Issue 3, "Radiation Shielding Policy," December 2023.

[36] Rolls-Royce SMR Limited, SMR0000512 Issue 1, "Radioactive Source Term Policy," July 2022.

[37] Rolls-Royce SMR Limited, SMR0000635 Issue 3, "Dose Management Policy," December 2023.

[38] Rolls-Royce SMR Limited, SMR0001861 Issue 2, "Radiation Protection Design Guidelines for the RR SMR," April 2024.

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

[40] Rolls-Royce SMR Limited, SMR0003984 Issue 5, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 5: Reactor Coolant Systems and Associated Systems," August 2025.

[41] Rolls-Royce SMR Limited, SMR0003929 Issue 4, "Environment, Safety, Security, and Safeguards Case Version 3, Tier 1, Chapter 7: Instrumentation and Control," August 2025.

[42] Rolls-Royce SMR Limited, SMR0004010 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 8: Electrical Power," August 2025.

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

[44] 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.

[45] Rolls-Royce SMR Limited, SMR0003880 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 10: Steam and Power Conversion Systems," August 2025.

[46] Rolls-Royce SMR Limited, SMR0004571 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 19: Emergency Preparedness and Response," August 2025.

[47] Rolls-Royce SMR Limited, SMR0009086 Issue 3, "ALARP Summary Report," May 2025.

[48] Rolls-Royce SMR Limited, C3.2.2-2, Conduct Design Optioneering.

[49] Rolls-Royce SMR Limited, C3.1.1, Define and Manage Requirements, June 2025.

[50] Rolls-Royce SMR Limited, SMR0003911 Issue 1, "Human Machine Interface (HMI) Style Guide," December 2022.

[51] Rolls-Royce SMR Limited, C3.2.2-4 Design for Conventional Safety Process, December 2023.

[52] Rolls-Royce SMR Limited, SMR0009412 Issue 1, "RD7 Reactor Island Layout - Requirements Summary," January 2024.

[53] Rolls-Royce SMR Limited, SMR0005054 Issue 1, "Codes and Standards for Mechanical Components of Safety Class 3 and Not Classified," September 2023.

[54] Rolls-Royce SMR Limited, SMR0008184 Issue 2, "Reactor Island Mechanical Handling Codes & Standards," February 2025.

[55] Rolls-Royce SMR Limited, SMR0004273 Issue 3, "C&I Codes and Standards Selection Report," January 2024.

[56] Rolls-Royce SMR Limited, SMR0006160 Issue 3, "Electrical Power System Codes and Standards," March 2025.

[57] Rolls-Royce SMR Limited, SMR0006030 Issue 2, "Civil and Structural Codes and Standards Policy," December 2024.

[58] Rolls-Royce SMR Limited, SMR0008678 Issue 1, "Codes for Aseismic Bearing Design Report," January 2025.

[59] Rolls-Royce SMR Limited, SMR0020199, Issue 1, "Demonstration of Practical Elimination of Large or Early Release," February 2025.

[60] Rolls-Royce SMR Limited, SMR0006357, Issue 1, "Phenomena Identification and Ranking Tables (PIRT) for Severe Accident Analysis," November 2023.

[61] IAEA, "Design Extension Conditions and the concept of Practical Elimination in the Design of NPPs, SSG-88," IAEA, Vienna, 2024.

[62] Rolls-Royce SMR Limited, SMR0000531 Issue 2, "Rolls-Royce SMR Deterministic Safety Case - Methodologies," January 2024.

[63] Rolls-Royce SMR Limited, SMR0006250 Issue 2, "Reactor Plant Performance Design Basis Analysis Methodology," November 2023.

[64] Rolls-Royce SMR Limited, SMR0005258 Issue 1, "Severe Accident Management Strategy," May 2023.
[65] Rolls-Royce SMR Limited, SMR0004735 Issue 2, "Probabilistic Safety Assessment Development Strategy," January 2024.
[66] Rolls-Royce SMR Limited, SMR0005205 Issue 1, "Rolls-Royce SMR Ageing Management Plan," April 2023.
[67] Rolls-Royce SMR Limited, SMR0008444 Issue 1, "Rolls-Royce SMR Approach to Verification and Validation," December 2023.
[68] Rolls-Royce SMR Limited, C3.2.3, Verify Design Definition, April 2025.
[69] Rolls-Royce SMR Limited, SMR0006518 Issue 2, "RR SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method," September 2024.
[70] Rolls-Royce SMR Limited, SMR0005548 Issue 2, "Identification of Environment Functions and Environmental Measures," July 2024.
[71] Office for Nuclear Regulation, "Security Assessment Principles for the Civil Nuclear Industry - Classified Annexes," Office for Nuclear Regulation, Bootle, United Kingdom, March 2022.
[72] Rolls-Royce SMR Limited, SMR0001391 Issue 2, "Rolls-Royce Small Modular Reactor Seismic Performance Classification Method," October 2022.
[73] Rolls-Royce SMR Limited, SMR0004542 Issue 4, "Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 2: Generic Site Characteristics," August 2025.
[74] Rolls-Royce SMR Limited, SMR0001535 Issue 3, "GB Generic Site Envelope," August 2024.
[75] Rolls-Royce SMR Limited, SMR0011147 Issue 1, "External Hazards Operating Basis Values," August 2024.
[76] Rolls-Royce SMR Limited, SMR0012746 Issue 1, "External Hazards Strategy," September 2024.
[77] Met Office, "UKCP18 User Interface," Met Office, Exeter, United Kingdom, 2018.
[78] Rolls-Royce SMR Limited, SMR0009084 Issue 2, "Combined External Hazards Report," 2025.
[79] Rolls-Royce SMR Limited, SMR0023526 Issue 1, "External Hazards Challenge Definition Report," 2025.
[80] Rolls-Royce SMR Limited, SMR0011081 Issue 1, "External-Internal Combined Hazards Methodology," 2025.
[81] Rolls-Royce SMR Limited, SMR0006070 Issue 3, "Generic Design Parameters for Civil Engineering," December 2024.
[82] Rolls-Royce SMR Limited, "EDNS01000888380 Design Input Spectra for UK Generic Design Assessment," April 2020.
[83] Rolls-Royce SMR Limited, SMR0017755 Issue 1, "RD8 Secondary Response Spectra Technical Note," April 2025.
[84] Rolls-Royce SMR Limited, SMR0005708 Issue 3, "Structural Design Method Statement for Safety Class 1 and 2 Structures," 2024.
[85] Rolls-Royce SMR Limited, SMR0011814 Issue 1, "Electromagnetic Interference Methodology and Identification," 2024.
[86] Rolls-Royce SMR Limited, SMR0005691 Issue 2, "Design Basis for Backup Generation Structures," 2023.
[87] Rolls-Royce SMR Limited, SMR0007038 Issue 2, "Analysis of Background Accidental Aircraft Crash Frequency," November 2023.
[88] Rolls-Royce SMR Limited, SMR0005709 Issue 3, "Aircraft Impact Design Philosophy and Methodology Statement," 2024.

[89] Rolls-Royce SMR Limited, SMR0008879 Issue 1, “Space Weather Hazard Methodology”.

[90] Rolls-Royce SMR Limited, SMR0005762 Issue 1, “National Grid (NG) Grid Code Compliance Strategy”.

[91] Rolls-Royce SMR Limited, SMR0009286 Issue 1, “System Design Description for the Low Voltage AC [BM] and DC [BP and BQ] Essential Uninteruptable Power Supply Systems,” November 2024.

[92] Rolls-Royce SMR Limited, SMR0012619 Issue 1, “System Design Description fro the Essential Electrical Supply Systems [BD, BK and BL],” October 2024.

[93] Rolls-Royce SMR Limited, SMR0020589 Issue 1, “Safety Measure Supply Sysem [KAX] - Water Supply Strategy,” 2025.

[94] Rolls-Royce SMR Limited, SMR0005529 Issue 1, “Internal Hazards Strategy,” April 2023.

[95] Rolls-Royce SMR Limited, SMR0012897 Issue 1, Internal Hazards Layout Reviews - Reactor Island.

[96] Rolls-Royce SMR Limited, SMR0006411 Issue 1, “Internal Hazards Methodology,” 2023.

[97] Rolls-Royce SMR Limited, SMR0013383, “Internal Hazards Analysis Report: EC&I Systems Block,” March 2025.

[98] Rolls-Royce SMR Limited, SMR0013786 Issue 1, “Internal Hazard Analysis Report: Auxilliary and Waste Blocks,” 2025.

[99] Rolls-Royce SMR Limited, SMR00141489 Issue 1, “Internal Hazards Analysis Report: Fuelling Block,” 2025.

[100] Rolls-Royce SMR Limited, SMR0013920 Issue 1, “Internal Hazards Internal Flooding Analysis,” 2024.

[101] Rolls-Royce SMR Limited, SMR0011210 Issue 1, “Internal Hazards Additional Fire Analysis Report - Impact on Civil Structures”.

[102] Rolls-Royce SMR Limited, SMR0013458 Issue 1, “Internal Hazards Local Fire Analysis Report”.

[103] Rolls-Royce SMR Limited, SMR0009446 Issue 1, “Internal Hazards within Hazard Shield Analysis Report”.

[104] Rolls-Royce SMR Limited, SMR0009983 Issue 1, “Internal Hazards Analysis - Outside Hazard Shield”.

[105] Rolls-Royce SMR Limited, SMR0023052 Issue 1, “Interim Hazards Schedule and Requirements for Design Reference Point 2,” May 2025.

[106] Rolls-Royce SMR Limited, SMR0008525 Issue 1, “Approach to Design Verification for Internal Hazards,” 2024.

[107] Rolls-Royce SMR Limited, SMR0007173 Issue 1, “Internal Combined Hazards Methodology and Identification Report,” 2023.

[108] Office for Nuclear Regulation, “Internal Hazards, ONR Technical Assessment Guide (TAG) NS-TAST-GD-014, Issue 7.1,” Office for Nuclear Regulation, Bootle, United Kingdom, December 2022.

[109] International Atomic Energy Agency, “Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.7,” International Atomic Energy Agency, Vienna, Austria, 2004.

[110] Building Regulations 2010, “Approved Document B (Fire Safety) volume 2: Buildings other than dwellings,” July 2019.

[111] British Standards Institution, “BS 9999:2017 Fire safety in the design, management and use of buildings. Code of practice”.

[112] Rolls-Royce SMR Limited, SMR0005825 Issue 1, “Site Fire Strategy Document,” June 2023.

[113] The National Archives, “The Dangerous Substances and Explosive Atmospheres Regulations 2002, United Kingdom Statutory Instrument 2002/2776,” The National Archives, 2002.

[114] British Standards Institution BS EN 60079, Explosive atmospheres, 2024.

[115] Center for Chemical Process Safety, Guidelines for Vapor Cloud Explosion, Pressure Vessel Burst, BLEVE, and Flash Fire Hazards, Wiley Online Library, July 2010.

[116] British Standards Institution BS EN IEC 6100, Electromagnetic compatibility (EMC), 2024.

[117] British Standards Institution BS EN IEC 62003, “Nuclear power plants – Instrumentation, control and electrical power systems – Requirements for electromagnetic compatibility testing,” British Standards Institution, 2020.

[118] The National Archives, “The Lifting Operations and Lifting Equipment Regulations 1998, United Kingdom Statutory Instrument 1998/2307,” The National Archives, London, United Kingdom, 1998.

[119] Health and Safety Executive, “Safe Use of Lifting Equipment, Lifting Operations and Lifting Equipment Regulations 1998, Approved Code of Practice and guidance. L113 Second Edition.,” The Stationery Office, London, United Kingdom, December 2014 (with amendments 2018).

[120] The National Archives, “The Provision and Use of Work Equipment Regulations 1998, United Kingdom Statutory Instrument 1998/2306,” The National Archives, London, United Kingdom, 1998.

[121] The National Archives, “The Control of Major Accident Hazards Regulations 2015, United Kingdom Statutory Instrument 2015/483,” The National Archive, London, United Kingdom, 2015.

[122] Rolls-Royce SMR Limited, SMR0021347 Issue 1, “Design inputs for Equipment Qualification framework,” May 2025.

[123] Rolls-Royce SMR Limited, SMR0008839 Issue 2, “Approach to Seismic Verification,” February 2025.

[124] Rolls-Royce SMR Limited, SMR0009111 Issue 2, “RR SMR EMIT Strategy,” December 2024.

[125] Rolls-Royce SMR Limited, SMR0022822 Issue 1, “Nuclear Safety SSC Classification Summary Report,” April 2025.

3.14 Appendix A: Postulated Initiating Events

Table 3.14-1: List of Postulated Initiating Events

RR SMR PIE	Applicable Operating Modes
Intact Circuit Faults	
ICF.1.1.01: Complete Loss of Pumped Primary Flow	1-4A
	4B-6A
ICF.1.1.02: Partial or Recoverable Loss of Pumped Primary Flow	1-4A
	4B-6A
ICF.1.1.03: Reactor Coolant Pump Shaft Seizure (Locked Rotor)	1-4A
ICF.1.2.01: Excessive Primary Pressure due to Spurious Initiation of Reactor Coolant Pump(s)	4B-5A
ICF.2.1.01: Primary Pressure Decrease due to Pressuriser Heaters Failing Off	1-5A
ICF.2.1.02: Primary Pressure Decrease due to Spurious Initiation of Pressuriser Spray	1-5A
ICF.2.2.01: Primary Pressure Increase due to Heaters Fail On	1-5A
ICF.2.2.02: Primary Pressure Increase due to Excessive Operation of Chemical Volume Control System	1-5A
ICF.2.2.03: Primary Pressure Increase due to Failure to Letdown	4A-5A
ICF.2.2.04: Excessive Primary Pressure due to Spurious Initiation of High Pressure Injection System	1-5B
ICF.3.1.01: Spurious Scram	1-2
ICF.3.1.02: Reactivity Control Imbalance	1-2
ICF.3.1.03: Spurious Initiation of Alternative Shutdown Function	1-2
ICF.3.2.01: Excessive Control Rod Withdrawal	1-2
	3-5B
ICF.3.2.02: Excessive Steam Demand due to Large Isolable Steam Leak	1-4A
ICF.3.2.03: Excessive Steam Demand due to Large Un-Isolable Steam Leak	1-4A
ICF.3.2.04: Excessive Steam Demand due to Steam Generator Rupture	1-4A
ICF.3.2.05: Temperature Reduction of Feedwater Supply	1-2
ICF.3.2.06: Excessive Steam Demand due to Spurious Steam Generator Relief Valve Lift	1-4A
ICF.3.2.07: Excessive Steam Demand due to Spurious Atmospheric Steam Dump	1-4A

RR SMR PIE	Applicable Operating Modes
ICF.3.2.08: Excessive Steam Demand due to Spurious High Temperature Heat Removal	1-4A
ICF.3.2.09: Excessive Withdrawal of Multiple Control Rod Banks	1-2
	3-5B
ICF.4.1.01: Complete Loss of Steam Generator Feed	2-4A
ICF.4.1.02: Partial Loss of Steam Generator Feed	1-4A
ICF.4.1.03: Loss of Duty Steam Generator Feed	1-4A
ICF.4.1.04: Un-isolable Feedwater Line Break	1-4A
ICF.4.2.01: Excessive Feedwater Supply	1-4A
ICF.5.1.01: Loss of Condenser	1-4A
ICF.5.1.02: Partial Loss of Secondary Heat Sink due to Partial Isolation of Steam Route to Condenser	1-4A
ICF.5.1.03: Turbine Trip	1
ICF.5.1.06: Spurious Containment Isolation	1-6B
ICF.5.2.01: Excessive Steam Demand due to Small Isolable Steam Leak	1-4A
ICF.5.2.02: Excessive Steam Demand due to Small Un-Isolable Steam Leak	1-4A
ICF.5.3.02: Partial or Recoverable Loss of Service Water System	1-6B
ICF.5.3.03: Inventory Loss from Service Water System	1-6B
Loss of Electrical Supply Faults	
LOE.1.0.00: Loss of Off-site Power (12 hours)	1-6B
LOE.1.0.01: Loss of Off-site Power (120 hours)	1-6B
LOE.1.0.02: Loss of Off-site Power (168 hours)	1-6B
LOE.1.0.03: Loss of Off-site Power (over 168 hours)	1-6B
LOE.1.1.01: Faulted Electrical Source Conditions	1-6B
LOE.2.1.01: Partial Loss of Station Electrical Supply	1-6B
LOE.2.1.02: Partial Loss of Essential Electrical Supply	1-6B
LOCAs	
LOC.0.1.01: Un-Isolable LOCA (Operator Dose)	3-6B
LOC.0.2.01: Isolable LOCA (Operator Dose)	1-6B
LOC.1.1.01: Small Un-Isolable LOCA	1-6B
LOC.1.2.01: Small Isolable LOCA	1-6B

RR SMR PIE	Applicable Operating Modes
LOC.2.1.01: Intermediate Un-Isolable LOCA	1-5A
	5B-6B
LOC.2.1.02: LOCA due to Single Steam Generator Tube Rupture	1-4A
LOC.2.1.03: LOCA due to Spurious Reactor Coolant System Relief Valve Lift	1-5A
LOC.2.1.04: Intermediate Un-Isolable LOCA due to Spurious Primary Blowdown	1-3
	4A-5A
LOC.2.1.05: Control Rod Drive Mechanism LOCA	1-5A
LOC.2.1.06: LOCA due to Double-ended Steam Generator Tube Rupture	1-4A
LOC.2.1.07: LOCA due to Multiple Steam Generator Tube Rupture	1-4A
LOC.2.2.01: Intermediate Isolable LOCA	1-6B
LOC.2.2.02: LOCA due to Cold Shutdown Cooling System Heat Exchanger Tube Rupture	4B-6B
LOC.2.2.03: LOCA due to Spurious Opening of Cold Shutdown Cooling System	1-4A
LOC.2.2.04: LOCA in Cold Shutdown Cooling System	4B-6B
LOC.3.1.01: Large Un-Isolable LOCA	1-5A
	5B-6B
LOC.3.1.02: LOCA due to Catastrophic Failure in Reactor Pressure Vessel	1-6B
Fuel Route and Mechanical Handling Faults	
REF.0.0.01: In-Containment Crane Collision	5B-6B
REF.0.0.02: Spent Fuel Pool Crane Collision	1-6B
REF.0.0.03: Core Collapse due to Mechanically Unstable Fuel Assemblies	6B
REF.0.0.04: Reactor Core Misload	6B
REF.1.0.01: Polar Crane Bridge / Trolley Collision with an Obstruction on the Rails	5B-6B
REF.1.0.02: Polar Crane Bridge / Trolley Overtravel	5B-6B
REF.1.0.03: Polar Crane Bridge / Trolley Skewing	5B-6B
REF.1.0.04: Polar Crane Bridge / Trolley Overspeed	5B-6B
REF.1.1.01: Polar Crane Main Hoist Double Blocking	5B-6B
REF.1.1.02: Polar Crane Main Hoist Snag and Drag	5B-6B
REF.1.1.03: Polar Crane Main Hoist Restrained Load	5B-6B
REF.1.1.04: Polar Crane Main Hoist Load Path Failure – Non-Arrestable	5B-6B
REF.1.1.05: Polar Crane Main Hoist Load Path Failure – Arrestable	5B-6B
REF.1.1.06: Polar Crane Main Hoist Uncontrolled Lowering	5B-6B

RR SMR PIE	Applicable Operating Modes
REF.1.1.07: Polar Crane Main Hoist Snag on Raising	5B-6B
REF.1.1.08: Polar Crane Main Hoist Ledge on Lowering	5B-6B
REF.1.1.09: Polar Crane Main Hoist Payload Collision	5B-6B
REF.1.1.10: Polar Crane Main Hoist Over-Raise of Irradiated Components	6B
REF.1.1.11: Inadvertent Withdrawal of one or more Control Rods during Reactor Pressure Vessel Upper Internals Lift	6A
REF.1.1.12: Polar Crane Main Hoist Overspeed	5B-6B
REF.1.2.01: Polar Crane Auxiliary Hoist Restrained Load	5B-6B
REF.1.2.02: Polar Crane Auxiliary Hoist Dropped Load	5B-6B
REF.1.2.03: Polar Crane Auxiliary Hoist Payload Collision	5B-6B
REF.1.2.04: Polar Crane Auxiliary Hoist Over-Raise of Irradiated Item	6B
REF.2.0.01: IC FHM Bridge / Trolley Collison with an Obstruction on Rails	6A-6B
REF.2.0.02: IC FHM Bridge / Trolley Overtravel	6A-6B
REF.2.0.03: IC FHM Bridge / Trolley Skewing	6A-6B
REF.2.1.01: IC FHM Main Hoist Double Blocking	6B
REF.2.1.02: IC FHM Main Hoist Snag and Drag	6B
REF.2.1.03: IC FHM Main Hoist Spurious Grab Disengagement	6B
REF.2.1.04: IC FHM Main Hoist Load Path Failure – Non-Arrestable	6B
REF.2.1.05: IC FHM Main Hoist Load Path Failure – Arrestable	6B
REF.2.1.06: IC FHM Main Hoist Uncontrolled Lowering	6B
REF.2.1.07: IC FHM Main Hoist Snag on Raising	6B
REF.2.1.08: IC FHM Main Hoist Ledge on Lowering	6B
REF.2.1.09: IC FHM Main Hoist Mast Seizure	6B
REF.2.1.10: IC FHM Main Hoist Payload Collision with Critical Infrastructure	6B
REF.2.1.11: IC FHM Main Hoist Payload Collision with Upender	6B
REF.2.1.12: IC FHM Main Hoist Over-Raise	6B
REF.2.2.01: IC FHM Auxiliary Hoist Restrained Load	6A-6B
REF.2.2.02: IC FHM Auxiliary Hoist Dropped Load	6A-6B
REF.2.2.03: IC FHM Auxiliary Hoist Collision	6A-6B
REF.2.2.04: IC FHM Auxiliary Hoist Over-Raise of Irradiated Item	6B
REF.3.0.01: SFP FHM Bridge / Trolley Collison with an Obstruction on Rails	1-6B
REF.3.0.02: SFP FHM Bridge / Trolley Overtravel	1-6B

RR SMR PIE	Applicable Operating Modes
REF.3.0.03: SFP FHM Bridge / Trolley Skewing	1-6B
REF.3.0.04: Fuel Assembly Stacking in Spent Fuel Pool	1-6B
REF.3.1.01: SFP FHM Main Hoist Double Blocking	1-6B
REF.3.1.02: SFP FHM Main Hoist Snag and Drag	1-6B
REF.3.1.03: SFP FHM Main Hoist Spurious Grab Disengagement	1-6B
REF.3.1.04: SFP FHM Main Hoist Load Path Failure – Non-Arrestable	1-6B
REF.3.1.05: SFP FHM Main Hoist Load Path Failure – Arrestable	1-6B
REF.3.1.06: SFP FHM Main Hoist Uncontrolled Lowering	1-6B
REF.3.1.07: SFP FHM Main Hoist Snag on Raising	1-6B
REF.3.1.08: SFP FHM Main Hoist Ledge on Lowering	1-6B
REF.3.1.09: SFP FHM Main Hoist Mast Seizure	1-6B
REF.3.1.10: SFP FHM Main Hoist Payload Collision with Critical Infrastructure	1-6B
REF.3.1.11: SFP FHM Main Hoist Payload Collision with Upender	1-6B
REF.3.1.12: SFP FHM Main Hoist Over-Raise	1-6B
REF.3.2.01: SFP FHM Auxiliary Hoist Restrained Load	1-6B
REF.3.2.02: SFP FHM Auxiliary Hoist Dropped Load	1-6B
REF.3.2.03: SFP FHM Auxiliary Hoist Payload Collision	1-6B
REF.3.2.04: SFP FHM Auxiliary Hoist Over-Raise of Irradiated Item	1-6B
REF.4.1.01: FTS Structural Failure	6B
REF.4.1.02: FTS Operation during Fuel Loading / Unloading	6B
REF.4.1.03: FTS Carriage Collision with Obstruction	6B
REF.4.1.04: FTS Carriage Overtravel	6B
REF.4.1.05: FTS Spurious Rotation and Travel	6B
REF.4.1.06: FTS Upender Over-Rotation	6B
REF.4.1.07: FTS Carriage Travel with Basket not Horizontal	6B
REF.4.1.08: FTS Fuel Assembly not Seated	6B
REF.4.1.09: FTS Fuel Assembly Falls Out of Basket	6B
REF.4.1.10: FTS Spurious Closure of Sealing Method	6B
REF.4.1.11: FTS Upender Seizure	6B
REF.4.1.12: FTS Upender Rotation with Inadequate Engagement	6B
REF.4.2.01: New Fuel Elevator Structural Failure	1-6B
REF.4.2.02: New Fuel Elevator Load Path Failure	1-6B

RR SMR PIE	Applicable Operating Modes
REF.4.2.03: New Fuel Elevator Basket Seizure	1-6B
REF.4.2.04: New Fuel Elevator Basket Over-Raise	1-6B
REF.4.2.05: New Fuel Elevator Basket Raises with Spent Fuel	1-6B
Spent Fuel Pool Faults	
SFP.1.1.02: Recoverable Loss of Duty Fuel Pool Cooling System	1-6B
SFP.2.1.01: LOCA in Fuel Pool Cooling System	1-6B
SFP.2.1.02: SFP Boundary LOCA During Fuel Shuffling	1-6A
SFP.2.1.03: SFP Boundary LOCA During Refuelling	6B
SFP.2.2.01: LOCA in Spent Fuel Pool Drain Line	1-6B
SFP.2.2.02: SFP Boundary LOCA During Cask Loading	1-6A
SFP.2.2.03: LOCA due to Catastrophic Failure of the Spent Fuel Pool	1-6B
SFP.3.1.01: Inadvertent Criticality in Spent Fuel Rack	1-6B
Internal Hazards	
INT.1.1.01: Fire in Containment	1-6B
INT.1.1.02: LOCA Conditions in Containment	1-6B
INT.1.1.03: Minor Disruptive Pipe Failure in Containment	1-5A
INT.1.1.04: Restrained Disruptive Pipe Failure in Containment	1-5A
INT.1.1.05: Catastrophic Pipe/Vessel Failure in Containment	1-2
INT.1.1.06: Reactor Coolant Pump Disintegration (Missiles)	1-4A
INT.1.1.07: Valve Stem Missiles in Containment	1-5A
INT.1.2.01: Fire in the Interspace	1-6B
INT.1.2.02: Steam Release/Flooding in Interspace	1-6B
INT.1.2.03: Accumulator Failure	1-4A
INT.1.2.04: Disruptive Pipe Failure of Main Steam Line	1-4A
INT.1.2.05: Other Infrequent Internal Hazard in Interspace	1-4A
INT.1.3.01: Fire in the Fuelling Block	1-6B
INT.1.3.02: Flooding in the Fuelling Block	1-6B
INT.1.3.03: Infrequent Hazard in Fuelling Block	1-6B
INT.1.4.01: Fire in Safety Fluids Block	1-6B
INT.1.4.02: Flood Originating in Safety Fluids Block	1-6B
INT.1.4.03: Infrequent Internal Hazard in Safety Fluids Block	1-6B
INT.1.5.01: Internal Hazard in Safety EC&I Block	1-6B

RR SMR PIE	Applicable Operating Modes
INT.1.6.01: Internal Hazard in Auxiliary Block	1-6B
INT.1.7.01: Internal Hazards in the Main Control Room	1-6B
INT.2.0.01: Internal Electromagnetic Interference	1-6B
INT.2.0.02: Hazardous Materials Affecting the Main Control Room	1-6B
INT.2.1.01: Turbine Disintegration	1
INT.2.1.02: Other Internal Hazards Outside the Hazard Shield	1-6B
External Hazards	
EXT.0.0.01: Accidental Aircraft Impact on Reactor & SFP Systems	1-6B
EXT.0.0.02: Storm Including Flooding Impact on Reactor & SFP Systems	1-6B
EXT.0.0.03: Earthquake Impact on Reactor & SFP Systems	1-6B
EXT.0.0.04: Tornadic Storm Impact on Reactor & SFP Systems	1-6B
EXT.0.0.05: Solar Activity Impact on Reactor & SFP Systems	1-6B
EXT.0.0.06: Cold Weather Impact on Reactor & SFP Systems	1-6B
EXT.0.0.07: Hot Weather Impact on Reactor & SFP Systems	1-6B
EXT.0.0.08: Industrial Hazards Impact on Reactor & SFP Systems	1-6B
EXT.0.1.01: Accidental Aircraft Impact on Intermediate Level Waste Systems	1-6B
EXT.0.1.02: Earthquake Impact on Intermediate Level Waste Systems	1-6B
EXT.0.1.03: Solar Activity Impact on Intermediate Level Waste Systems	1-6B
EXT.0.1.04: Other External Hazards Impact on Intermediate Level Waste Systems	1-6B
EXT.0.2.01: External Hazards Impact on Interim Stores	1-6B
EXT.0.3.01: External Hazards Impact on Low Level Radiation Storage	1-6B
Non-Fuel Melt Faults	
NFM.0.0.02: Operator Exposure	1-6B
NFM.1.1.04: Release from Liquid Retentate System	1-6B
NFM.1.2.01: Release from Gaseous Waste System	1-6B
NFM.1.3.01: Release from Solid Waste Storage	1-6B
NFM.1.3.02: Release from Solid Waste Processing Systems	1-6B
NFM.1.3.03: Overfill of Solid Waste Storage	1-6B
NFM.1.4.01: Release from High-Activity Liquid Effluent System	1-6B
NFM.1.4.02: Overfill of Non-Vented High-Activity Liquid Effluent System	1-6B
NFM.1.4.03: Overfill of KNF10 Tank	1-6B
NFM.1.4.04: Overfill of KTA20 Tank	1-6B

RR SMR PIE	Applicable Operating Modes
NFM.1.4.05: Overfill of KNF Retentate Tank	1-6B
NFM.1.5.01: Release from Low-Activity Liquid Effluent System	1-6B
NFM.1.5.02: Release of Airborne Contamination from Contaminated Item Storage/Handling	1-6B
NFM.2.1.01: Inadvertent Operator Exposure to R3 Area	1-6B
NFM.2.1.02: Inadvertent Operator Exposure to R4 Area	1-6B
NFM.2.1.03: Inadvertent Operator Exposure to R5 Area	1-6B
NFM.2.1.04: Inadvertent Operator Exposure to R5 Bunker Area	1-6B

3.15 Appendix B: Summary of SSC Classification

Table 3.15-1 is populated with classifications that are assigned to SSCs, noting:

- EM = Environmental Measure.
- KSE = Key Safeguards Equipment.
- None = Assessment at DRP4 indicates no classification.
- TBD = No assessment has been undertaken at DRP4 and the classification is to be determined, or initial assessment has been undertaken and confirmation is still required. These will continue to be populated in future versions of the generic E3S Case as SSC classifications continue to be confirmed and assigned through the design process.

An SSC may attract different classifications to different parts of it, and this table presents the highest or majority classification for each SSC, noting the following exceptions [125]:

- (*) means that a system that is mainly classified a safety class 2 or 3 also has safety class 1 containment isolation valves.
- (#) means that a system that is mainly classified as safety class 2 or 3 also has safety class 1 isolation valves (for reasons other than containment isolation).
- (^) means that a system that is mainly classified as safety class 3 or not classified also has safety class 2 isolation valves.

Table 3.15-1: Summary of SSC Classification

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
RO1	**REACTOR ISLAND**						
J	Reactor Plant						
JA	Reactor System						
JAA	Reactor Vessel System	1 (VHR)	EM	None	KSE	SPC1	
JAC	Reactor Core System	1	EM	None	KSE	SPC1	
JD	Reactor Reactivity Control Systems						
JD01	Scram Safety Measure	1	None	None	None	SPC1	
JD02	Alternative Shutdown Function Safety Measure	2	None	None	None	SPC1	
JD03	Rapid Power Reduction	3	None	None	None	TBD	
JD04	Duty Reactivity Control	3	None	None	None	SPC3	
JDK	Emergency Boron Injection System	2	None	None	None	SPC1	
JE	Reactor coolant system						
JEA	Steam Generation System	1 (VHR)	EM	None	None	SPC1	
JEB	Reactor Coolant Pump System	1 (VHR)	EM	None	None	SPC1	
JEC	Reactor Coolant Pipework System	1 (some VHR)	EM	None	None	SPC1	
JEF	Reactor Coolant Pressurising System	1 (VHR)	EM	None	None	SPC1	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
JEG	Reactor Coolant Pressure Relief System	1	EM	None	None	SPC1	
JK	Core Instrumentation Systems						
JKQ	In-Core Calibration System	3	None	TBD	KSE	TBD	
JKS	In-Core Monitoring System	TBD	None	TBD	KSE	TBD	
JKT	Ex-Core Monitoring System	1	None	TBD	KSE	SPC1	
JM	Reactor Plant Containment Systems						
JM01	Faulted Containment Safety Measure	1	None	3	None	SPC1	
JM02	Severe Accident Containment Safety Measure	3	None	None	KSE	SPC1	
JMA	Containment System	1	EM	3	None	SPC1	
JMT	Hydrogen Reduction System	2	EM	None	None	SPC1	
JN	Reactor Heat Removal Systems						
JN01	Emergency Core Cooling Safety Measure	1	None	None	None	SPC1	
JN02	Passive Decay Heat Removal Safety Measure	2	None	None	None	SPC1	
JN03	Condenser Decay Heat Removal	3	None	None	None	SPC3	
JN04	Low Temperature Decay Heat Removal	2	None	None	None	SPC1	
JNA	Cold Shutdown Cooling System	2 (*)	None	None	None	SPC1	
JNB	Passive Steam Condensing System	2 (*)	None	None	None	SPC1	
JND	High Pressure Injection System	2 (*)	None	None	None	SPC1	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
JNF	Automatic Depressurisation System	1	None	None	None	SPC1	
JNG	Low Pressure Injection System	1	None	None	None	SPC1	
JNH	In Containment Water Storage System	1	None	None	None	SPC1	
JNK	Local Ultimate Heat Sink System	1	None	None	None	SPC1	
JNM	Reactor Vessel Cavity Injection System	3 (#)	None	None	None	SPC1	
JQ	Diverse Protection System						
JQA	Diverse Protection System	1	None	None	None	SPC1	
JR	Reactor Protection and Accident Management System						
JRA	Reactor Protection System	1	None	None	None	SPC1	
JRQ	Accident Management System	1	None	None	KSE	SPC1	
JS	Reactor Plant Control and Monitoring System						
JSA	Reactor Plant Control System	3	None	None	None	SPC3	
JSS	Reactor Monitoring System	None (TBD)	None	None	KSE	None (TBD)	
F	Handling of Nuclear Equipment						
FA	Internal Storage of Fuel Assemblies and Other Radioactive Parts						
FA01	Fuel Pool Boil Off	1	None	None	None	SPC1	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
FA02	Faulted Fuel Pool Cooling	2	None	None	None	SPC1	
FA03	Safe, Moderated, Absorbers, Unrodded, Geometry	1	None	None	None	SPC1	
FA03	Safe, Moderated, Unrodded, Geometry	1	None	None	None	SPC1	
FAA	New Fuel Receipt and Inspection Area	1 (TBD)	EM	None	KSE	SPC1 (TBD)	
FAB	Spent Fuel Storage and Cask Loading	1	EM	None	KSE	SPC1	
FAE	Refuelling Cavity	1	EM	None	KSE	SPC1	
FAF	Refuelling Pool	1	EM	None	KSE	SPC1	
FAK	Fuel Pool Cooling System	2 (*,#)	EM	None	None	SPC1	
FAL	Fuel Pool Purification System	3 (TBD)	EM	None	None	SPC3 (TBD)	
FAN	Fuel Pool Venting system	1	EM	None	None	SPC1	
FAT	Fuel Pool Supply System	3 (TBD)	EM	None	None	TBD	
FB	Handling of fuel assemblies and other reactor core internals						
FBA	Testing System for Fuel Assemblies (also includes reflector assemblies)	TBD	EM	3 (TBC)	KSE	TBD	
FC	Refuelling and Conveyance System for Fuel and other Reactor Core Internals						

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
FCD	Cask Loading System	1 (TBD)	EM	None	KSE	SPC1 (TBD)	
FCJ	System for Conveyance of Fuel Assemblies/ Internals within Reactor Area	1	EM	None	KSE	SPC1	
FCK	System for Conveyance of Fuel Assemblies/ Internals Between Reactor and Storage Areas	1 (TBD)	EM	None	KSE	SPC1 (TBD)	
FCL	System for Conveyance of Fuel Assemblies/ Internals within Storage Area	1 (TBD)	EM	None	KSE	SPC1 (TBD)	
FD	External Storage of Spent Fuel						
FDB	External Dry Storage of Filled Casks	1	EM	None	KSE	SPC1	
FDC	Inspection System for Casks in External Storage	None (TBD)	EM	None	KSE	SPC3 (TBD)	
FJ	Erection or In-Service Inspection System						
FJA	Tools and Erection System for Reactor Vessel (including Closure Head)	TBD	None	TBD	KSE	TBD	
FJB	Tools and Erection System for Reactor Vessel Internals	None (TBD)	None	TBD	KSE	SPC3 (TBD)	
FJC	In-Service Inspection System for the Reactor Vessel (and Closure Head)	TBD	None	TBD	KSE	TBD	
FJD	In-Service Inspection System for Reactor Vessel Internals	None (TBD)	None	TBD	KSE	SPC3 (TBD)	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
FK	Decontamination System						
FKA	Component Decontamination System	3 (TBD)	EM	None	KSE	SPC 3 (TBD)	
FKB	Poolside Equipment Decontamination System	3 (TBD)	EM	None	KSE	TBD	
FY	Fuel Route C&I						
FYB	Fuel Route C&I System	2	EM	None	KSE	SPC1	
FYC	Fuel Route C&I System	3	EM	None	KSE	SPC3	
FYS	Fuel Route C&I System	1	EM	None	KSE	SPC1	
FYT	IAEA Safeguards	None	None	None	KSE	SPC3	
K	Nuclear Auxiliary Systems						
KA	Component Cooling Systems						
KAA	Component Cooling System	2 (*)	None	None	None	SPC1	
KAX	Safety Measure Coolant Supply Subsystem	3 (*)	None	None	None	SPC1	
KB	Chemical and Volume Control System						
KBA	Level and Volume Control System	3	EM	None	None	SPC3 (TBD)	
KBD	Chemistry Control System	3 (TBD)	EM	None	None	SPC3 (TBD)	
KBE	Coolant Purification System	3 (TBD)	EM	None	None	TBD	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
KH	Nuclear Heat Tracing Systems						
KHA	Heat Tracing System for Reactor Coolant System	TBD	None	TBD	None	TBD	
KHB	Heat Tracing System for Secondary Coolant System	TBD	None	TBD	None	TBD	
KHC	Heat Tracing System for other systems	TBD	None	TBD	None	TBD	
KJ	Reactor Island Chilled Water System						
KJA	Endurance Period Cooling System	1	None	None	None	SPC1	
KJL	Normal Operation Chilled Water and Heating System	2	EM	None	None	SPC1	
KL	Reactor Island HVAC System						
KLA	HVAC Systems serving Primary Containment	3 (*)	EM	None	None	SPC3	
KLB	HVAC Systems serving the Interspace and Outage area	3 (TBD)	EM	None	None	SPC3 (TBD)	
KLC	HVAC Systems serving the Fluid Blocks	2	EM	None	None	SPC1	
KLE	HVAC Systems serving Uncontrolled Areas	1	None	None	None	SPC1	
KLF	HVAC Systems serving Radioactive Waste Processing areas	2 (TBD)	EM	None	None	SPC1 (TBD)	
KLL	HVAC Systems serving Fuel Storage and Handling Areas	3 (TBD)	EM	None	None	SPC3 (TBD)	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
KLQ	Controlled Areas HVAC Common Supply and Extract Plant	3 (TBD)	EM (TBD)	None	None	SPC3 (TBD)	
KLR	HVAC Systems serving the Control Rooms	1 (TBD)	None	None	None	SPC1	
KLS	HVAC Extract System Discharge System	TBD	EM (TBD)	None	None	TBD	
KM	Solid Radioactive Waste Management system						
KMA	Solid Radioactive Waste Processing System	3	EM	None	None	TBD	
KME	Solid Radioactive Waste Storage System	3	EM	None	None	TBD	
KN	Liquid Radioactive Effluent Treatment System						
KNF	Liquid Radioactive Effluent Treatment System	3	EM	None	None	TBD	
KP	Gaseous Radioactive Effluent Treatment system						
KPL	Gaseous Radioactive Effluent Treatment system	3 (TBD)	EM	None	None	TBD	
KT	Collection and Drainage systems for liquid media in controlled and exclusion areas						
KTA	Reactor Island Collection and Drainage System	3 (TBD)	EM	None	None	TBD	
KTQ	Fuel Pools Leak Detection & Collection System	3	EM	None	None	SPC3	
KU	Reactor Coolant Sampling System						

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
KUA	Nuclear Sampling System	3 (*) (TBD)	EM	None	None	TBD	
KUB	Auxiliary Sampling System	TBD	EM	None	None	TBD	
KUK	Process & Emissions Radiation Monitoring System	TBD	EM	None	None	TBD	
KY	Radioactive Waste Management System C&I						
KYA	Radioactive Waste Management System C&I	3	EM	None	KSE	SPC3	
KYQ	Radioactive Waste Management System C&I	2	EM	None	KSE	SPC1	
TO1	**TURBINE ISLAND**						
L	Steam Water Condensate System						
LA	Feedwater System	3	None	TBD	None	SPC3 (TBD)	
LB	Steam System	1 [R01] 3 [T01]	None	TBD	None	SPC1 [R01] SPC3 [T01]	
LC	Condensate System	3	EM (TBD)	TBD	None	SPC3 (TBD)	
LD	Condensate Polishing System	3	EM	TBD	None	SPC3 (TBD)	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
LJ	Auxiliary Feedwater Supply System	3	None	TBD	None	SPC3 (TBD)	
LX	Fluid supply systems for control and protection systems	3	None	TBD	None	SPC3 (TBD)	
LY	Control and Protection Systems - Feedwater, Steam & Condensate	3	None	TBD	None	TBD	
M	Main Turbine Generator System						
MA	Steam Turbine System	3	EM (TBD)	TBD	None	SPC3 (TBD)	
MK	Generator System	3	EM (TBD)	TBD	None	SPC3 (TBD)	
MS	Generator Transmission Main Connection	3	EM	TBD	None	SPC3 (TBD)	
MU	Common Systems of the Main Turbine Generator System	3	None	TBD	None	SPC3 (TBD)	
MY	Control and Protection Systems Turbine Island	TBD	None	TBD	None	TBD	
CO1	**COOLING WATER ISLAND**						
P	Cooling Water Systems						
PA	Main Cooling Water System	3	EM (TBD)	None	None	SPC3	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
PB	Essential Service Water System	2	EM (TBD)	None	None	SPC1	
PE	Auxiliary Cooling and Make-up System	3	EM (TBD)	TBD	None	SPC3	
PF	Shared Cooling Water System	3	EM (TBD)	TBD	None	SPC3	
PG	Turbine Island Closed Cooling Water System	3	EM (TBD)	TBD	None	SPC3	
PU	Common Systems for the Cooling Water System	3	EM (TBD)	TBD	None	SPC3	
PY	Control and Protection System Cooling Water Island	TBD	EM (TBD)	TBD	None	TBD	
BO1	**Balance of Plant – Main System**						
G	Water Supply - Disposal and Treatment System						
GA	Water Supply System	3 (TBD)	EM (TBD)	TBD	None	SPC3	
GC	Demineralization Treatment System	None (TBD)	EM	TBD	None	SPC3	
GH	Treated Water Distribution System	None (^) (TBD)	EM	TBD	None	SPC3	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
GM	Waste Water Drainage and Treatment Systems	None (TBD)	EM (TBD)	TBD	None	SPC3	
Q	Auxiliary Systems						
QC	Chemicals Supply System	None (TBD)	EM (TBD)	TBD	None	SPC3	
QF	Central Control Air Supply System	None (TBD)	EM (TBD)	TBD	None	SPC3	
QH	Auxiliary Steam Generating System	None (TBD)	None	TBD	None	SPC3	
QJ	Central Gas Supply System	None (TBD)	EM (TBD)	TBD	None	SPC3	
QU	Auxiliary Non-Nuclear Sampling System	None (TBD)	EM (TBD)	TBD	None	SPC3	
V	Systems for Storage of Materials or Goods						
W	Systems for Administrative or Social Purposes or Tasks						
X	Ancillary Systems						
XA	Non-Nuclear Ventilation and Air-Conditioning System	None (TBD)	EM (TBD)	TBD	None	SPC3	
XB	Heating System	None (TBD)	None	TBD	None	SPC3	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
XD	Cleaning Systems (excluding nuclear)	None (TBD)	None	TBD	None	SPC3	
XE	Welding Gas Systems	None (TBD)	None	TBD	None	SPC3	
XF	Earthing and Lightning Protection System	TBD	None	TBD	None	TBD	
XG	Fire Extinguishing System	3(TBD)	EM	TBD	None	SPC3	
XJ	Mobile system for people and material transport	None (TBD)	None	TBD	None	SPC3	
XK	Chilled Water System	None (TBD)	None	TBD	None	SPC3	
XM	Mechanical Handling System	None (TBD)	None	TBD	None	SPC3	
XQ	Lighting Systems	None (TBD)	None	TBD	KSE	SPC3	
XR	Systems for workshops and laboratories in nuclear controlled area	None (TBD)	EM	TBD	None	SPC3	
XS	Safety Services	None (TBD)	None	3 (TBD))	None	SPC3	
XT	Systems for factory, petrol station, garage and laboratory (excluding nuclear controlled and exclusion area)	None (TBD)	None	TBD	None	SPC3	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
XU	Sanitary Wastewater System	None (TBD)	EM (TBD)	TBD	None	SPC3	
XV	Rainwater System	None (TBD)	EM (TBD)	TBD	None	SPC3	
E01	**Electrical, Control and Instrumentation Systems - Main System**						
A	Grid Transmission System						
AC	400kV Grid Transmission Connection System	3	None	TBD	KSE	SPC3	
B	Electrical Power System						
BB	High Voltage Main AC Supply System	3	None	TBD	KSE	SPC3	
BC	High Voltage Main AC Standby Supply System	3	None	TBD	KSE	SPC3	
BD	High Voltage Essential AC Standby Supply System	2	EM (TBD)	None	KSE	SPC1	
BF	Low Voltage Main AC Supply System for Process Equipment	3	None	TBD	KSE	SPC3	
BG	Low Voltage Main AC Supply System for Non-Process Equipment	3	None	TBD	KSE	SPC3	
BK	Low Voltage Essential AC Standby Supply System	2	EM (TBD)	None	KSE	SPC1	
BL	Low Voltage Essential AC Alternate Supply System	2	EM (TBD)	TBD	KSE	SPC1	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
BM	Low Voltage Uninterruptible AC Supply System	2	None	TBD	KSE	SPC1	
BP	Low Voltage Uninterruptible DC Supply System	3	None	TBD	KSE	SPC1	
BQ	Low Voltage Uninterruptible DC Supply System for Safety Services	1	None	None	KSE	SPC1	
BY	Electrical Power System Control and Instrumentation	1 (TBD)	None	TBD	KSE	SPC1 (TBD)	
C	Control and Management Systems						
CA	HVAC C&I Systems	1 (TBD)	EM	TBD	None	SPC1 (TBD)	
CB	Data Processing and Control System	3 (TBD)	None	TBD	KSE	SPC3 (TBD)	
CC	Upper-Level Automation System	3 (TBD)	None	TBD	None	SPC3 (TBD)	
CD	Diagnostic Systems	3 (TBD)	None	TBD	None	SPC3 (TBD)	
CE	Engineering Systems	TBD	None	TBD	None		
CF	Data transfer and remote-control system	None (TBD)	None	TBD	None	SPC3 (TBD)	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
CJ	Optimisation - Plant Simulators	None (TBD)	None	TBD	None	SPC3 (TBD)	
CK	Process Monitoring	3 (TBD)	EM (TBD)	TBD	None	SPC3 (TBD)	
CM	Plant Management Software	3 (TBD)	None	TBD	KSE	SPC3 (TBD)	
CP	Fire Systems - C&I	3 (TBD)	None	TBD	None	SPC3 (TBD)	
CQ	Control Room Equipment	3 (TBD)	None	3 (TBD)	KSE	SPC3 (TBD)	
CR	Radiation Monitoring System	2 (TBD)	None	TBD	None	SPC1	
CU	Building Systems Control	None (TBD)	None	TBD	None	SPC3 (TBD)	
Y	Communication and Information Systems						
YA	Communications Systems	TBD	None	TBD	KSE	TBD	
YB	Information Systems	TBD	None	TBD	KSE	TBD	
YC	Information Technology	TBD	None	TBD	KSE	TBD	
SO1	**Civil, Structural and Architectural – Main Systems**						

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
U	Structures and Areas for Systems inside of the Power Plant Process						
U01	Reactor Island Structures and Areas						
UA	Structures and Areas for Electrical Grid and Distribution System						
UAB	Structures and areas for transforming, converting and switching systems	3	None	TBD	None	SPC3 (TBD)	
UB	Structures for Electrical Auxiliary Power Supply System						
UBB	Structures for Common Electrical and C&I Systems	3	None	TBD	None	SPC3	
UBM	Back-up Generation Structures	2	EM (TBD)	TBD	None	SPC1	
UF	Structures for the Handling of Nuclear Equipment						
UFA	Structures for Fuel Storage	1	EM (TBD)	None	None	SPC1	
UG	Structures for Water Supply/Disposal and Treatment						
UGA	Structure for Raw Water Supply	None (TBD)	None	TBD	None	SPC3 (TBD)	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
UGC	Structure for Treatment by Demineralization	None (TBD)	EM (TBD)	TBD	None	SPC3 (TBD)	
UGN	Structure for Process Drains Treatment System	None (TBD)	EM (TBD)	TBD	None	SPC3 (TBD)	
UJ	Structures for Reactor Plant						
UJA	Containment Internal Structures	1	EM	3 (TBD)	None	SPC1	
UJB	Structures for Interspace	1	None	3 (TBD)	None	SPC1	
UJQ	Containment Support Structure	1	None	3 (TBD)	None	SPC1	
UJS	Structures for EC&I Systems	1	None	3 (TBD)	None	SPC1	
UJT	Structures for Fluid Systems	2 (TBD)	EM (TBD)	3 (TBD)	None	SPC1	
UK	Structures for Reactor Auxiliary Systems						
UKA	Structures for Auxiliary Systems	1	EM (TBD)	TBD	None	SPC1	
UKB	Structures for Access & Ancillary Systems	2 (TBD)	None	TBD	None	SPC1 (TBD)	
UKH	Structure for Air Exhaust	3 (TBD)	EM	TBD	None	SPC2 (TBD)	
UKQ	Structures for Outage Activities	3 (TBD)	None	TBD	None	SPC2 (TBD)	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
UKT	Structure for Radioactive Waste Storage	3 (TBD)	EM	TBD	None	SPC2 (TBD)	
UM	Structures for systems for conversion of energy and for transmission of electrical energy						
UMA	Turbine Hall	3 (TBD)	None	TBD	None	SPC2 (TBD)	
UMB	Turbine Hall Electrical Annexes	3	None	TBD	None	SPC3	
UMS	Structure for Transmission of Electrical Energy	3	None	TBD	None	TBD	
UP	Structures for Cooling Water Systems						
UPC	Structures for Cooling Water Conveyance	3	EM (TBD)	TBD	None	SPC3	
UPD	Structure for Cooling Water Intake and Supply (Auxiliary and Secondary Processes)	3	EM (TBD)	TBD	None	SPC3	
UPE	Structure for Cooling Water Mechanical Cleaning (Auxiliary and Secondary Processes)	3	EM (TBD)	TBD	None	SPC3	
UPF	Structures for Auxiliary Cooling & Make-up System	3	EM (TBD)	TBD	None	SPC3	
UPG	Structures for Main Cooling Water System - Cooling Tower System	3	EM (TBD)	TBD	None	SPC3	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
UPJ	Structures for Essential Services Water System	3	EM (TBD)	TBD	None	SPC3	
UPK	Structure for Cooling Water Recirculation and Outfall Cooling System	3	EM	TBD	None	SPC3	
UPN	Structure for Biocide Preparation and Cooling Water Biocide Treatment	3	EM (TBD)	TBD	None	SPC3	
UQ	Structures for Auxiliary Systems						
UQC	Structure for Central Chemical Supply	None (TBD)	EM (TBD)	TBD	None	SPC3 (TBD)	
UQF	Structure for Central Control Air Supply	None (TBD)	EM (TBD)	TBD	None	SPC3 (TBD)	
UQH	Structure for Auxiliary Steam Generation	None (TBD)	EM (TBD)	TBD	None	SPC3 (TBD)	
UW	Structures for Common Systems						
UWC	Foundations, Retaining Structures and Seismic Isolation	1	None	3 (TBD)	None	SPC1	
UWD	Hazard Shield and Basemat	1	None	3 (TBD)	None	SPC1	
UX	Modularisation Kit of Parts System						
UXA	Primary Structures	TBD	None	TBD	None	TBD	
UXB	Barriers	TBD	None	TBD	None	TBD	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
UXC	Civil and Structural Interfacing Structures	TBD	None	TBD	None	TBD	
UXD	Ancillary Structures	TBD	None	TBD	None	TBD	
UXZ	SMR Product Assemblies (Non-Functional)	TBD	None	TBD	None	TBD	
Z	Structures and Areas for Systems Outside of the Power Plant Process						
ZV	Structures and Surfaces for Storage of Material and Goods	TBD	None	TBD	None	TBD	
ZX	Structures for Ancillary Systems	TBD	EM (TBD)	TBD	None	TBD	
ZY	Structures for Communications and Information	TBD	None	TBD	None	TBD	
ZT	Temporary Works	TBD	EM (TBD)	TBD	None	TBD	
ZW	Structures for Administrative Tasks or Staff Amenities	TBD	None	3 (TBD)	None	TBD	
ZZ	Structures and Surfaces for conveyance and traffic, fencing, gardens and other purposes	TBD	EM (TBD)	TBD	None	TBD	

3.16 Abbreviations

AAC	Accidental Aircraft Crash
AC	Alternating Current
ACoP	Approved Code of Practice
ADB	Approved Document B
ADS	Automatic Depressurisation System
AHU	Air Handling Unit
ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
AMP	Ageing Management Plan
ASD	Atmospheric Steam Dump
ASF	Alternative Shutdown Function
ASME	American Society of Mechanical Engineers
ATEX	Directive 99/92/EC and Directive 2014/34/EU
BAT	Best Available Techniques
BLEVE	Boiling Liquid Expanding Vapour Explosion
BS	British Standard
BSL	Basic Safety Level
BSO	Basic Safety Objective
BUGS	Back-Up Generator System
C&I	Control and Instrumentation
CAE	Claims, Arguments, Evidence
CCF	Common Cause Failure
CCPS	Center for Chemical Process Safety
CCS	Component Cooling System
CDF	Core Damage Frequency
CET	Core Exit Temperature
CFD	Computational Fluid Dynamics
CfT	Categorisation for Theft
CIV	Containment Isolation Valve
CKoP	Civils Kit of Parts
CLP	Cask Loading Pit

CoFT	Control of Fuel Temperature
COMAH 2015	Control of Major Accident Hazards Regulations 2015
CoR	Control of Reactivity
CoRE	Control of Radiation Exposure
CoRM	Confinement of Radioactive Material
CPS	Cyber Protection System
CRDM	Control Rod Drive Mechanism
CSCS	Cold Shutdown Cooling System
CSRA	Cyber Security Risk Assessment
CV	Containment Vessel
DBC	Design Basis Condition
DBE	Design Basis Earthquake
DBT	Design Basis Threat
DC	Direct Current
DCH	Direct Containment Heating
DEC	Design Extension Condition
DG	Diesel Generator
DHR	Decay Heat Removal
DiD	Defence in Depth
DIS	Design Input Spectra
DNBR	Departure from Nucleate Boiling Ratio
DPS	Diverse Protection System
DRP4	Design Reference Point 4
DSEAR 2002	Dangerous Substances and Explosive Atmospheres Regulations 2002
E3S	Environment, Safety, Security and Safeguards
EA	Environment Agency
ECC	Emergency Core Cooling
EH	External Hazard
EM	Environmental Measure
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMIT	Examination, Maintenance, Inspection and Testing
EN	Euronorm

EPRI	Electric Power Research Institute
EQ	Equipment Qualification
ERP	Emergency Response and Plans
ESWS	Essential Service Water System
EU	European Union
EUR	European Utility Requirements
FBOM	Functional Bill of Materials
FDT	Fire Dynamic Tools
FE	Finite Element
FHM	Fuel Handling Machine
FPBO	Fuel Pool Boil-Off
FPC	Fuel Pool Cooling
FPVS	Fuel Pool Venting System
FSF	Fundamental Safety Function
GALL	Generic Ageing Lessons Learned
GB	Great Britain
GSE	Generic Site Envelope
HAZID	Hazard Identification
HEAF	High Energy Arcing Fault
HLSF	High-Level Safety Function
HMI	Human-Machine Interface
HPME	High Pressure Melt Ejection
HR	High Reliability
HRR	Heat Release Rate
HRS	Hydrogen Reduction System
HTHR	High Temperature Heat Removal
HTOP	High Temperature Overpressure-Protection
HV	High Voltage
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICF	Intact Circuit Fault

ICRP	International Commission on Radiological Protection
IEF	Initiating Event Frequency
IEMO	Initiating Event of Malicious Origin
IH	Internal Hazard
IHP	Integrated Head Package
IRR 2017	Ionising Radiations Regulations 2017
ISI	In-Service Inspection
IST	In-Service Testing
IVR	In-Vessel Retention
IWSS	In-Containment Water Storage System
KEPE	Key Environmental Protection Equipment
KOH	Potassium Hydroxide
KSE	Key Safeguards Equipment
LOCA	Loss of Coolant Accident
LOLER 1998	Lifting Operations and Lifting Equipment Regulations 1998
LOOP	Loss of Off-site Power
LOOW	Loss of Off-site Water
LPS	Lightning Protection System
LRF	Large Release Frequency
LTDHR	Low Temperature Decay Heat Removal
LUHS	Local Ultimate Heatsink System
LV	Low Voltage
MCCI	Molten Corium Concrete Interaction
MCR	Main Control Room
MCWS	Main Cooling Water System
MEP	Mechanical, Electrical and Plumbing
MKoP	Modular Kit of Parts
N/A	Not Applicable
NFCC	Non-Fuel Core Component
NFE	New Fuel Elevator
NFS	New Fuel Store

NIST	National Institute of Science and Technology
NMACS	Nuclear Material Accountancy, Control and Safeguards
NRC	Nuclear Regulatory Commission
O&M	Operation and Maintenance
OBE	Operating Basis Earthquake
OLC	Operational Limit and Condition
ONR	Office for Nuclear Regulation
OPEX	Operating Experience
pa	Per Annum
PAR	Passive Autocatalytic Recombiner
PDHR	Passive Decay Heat Removal
PDS	Plant Damage State
PGA	Peak Ground Acceleration
PIE	Postulated Initiating Event
PIRT	Phenomena Identification and Ranking Table
PPS	Physical Protection System
PSA	Probabilistic Safety Assessment
PUWER 1998	Provision of Use of Work Equipment Regulations 1998
PWR	Pressurised Water Reactor
RAIDO	Risks, Assumptions, Issues, Dependencies and Opportunities
RCS	Reactor Coolant System
RFI	Radio Frequency Interference
RGP	Relevant Good Practice
RICW	Reactor Island Chilled Water
RPCS	Reactor Protection Control System
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RRC	Radiological Release Category
RR SMR	Rolls-Royce Small Modular Reactor (the design)
RVCIS	Reactor Vessel Cavity Injection System
SA	Severe Accident

SAA	Severe Accident Analysis
SAD	Severe Accident Depressurisation
SAMG	Severe Accident Management Guideline
SAMS	Severe Accident Management System
SAP	Safety Assessment Principle
SBO	Station Blackout
SbyD	Secure by Design
SDD	System Design Description
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SIS	Seismic Isolation System
SMAUG	Safe, Moderated, Absorbers, Unrodded, Geometry
SMDD	Safety Measure Design Description
SMUG	Safe, Moderated, Unrodded, Geometry
SPC	Seismic Performance Class
SRS	Secondary Response Spectra
SSC	Structure, System and Component
SyAP	Security Assessment Principle
TAG	Technical Assessment Guide
TBD	To Be Decided
TH	Time History
TLA	Through-Life Activity
UK	United Kingdom
UKCP18	UK Climate Projections 2018
UPS	Uninterruptible Power Supply
US	United States of America
V&V	Verification and Validation
VAI&C	Vital Area Identification And Categorisation
VCE	Vapour Cloud Explosion
VTA	Vehicular Transport Accident

WENRA	Western European Nuclear Regulators' Association
Yr	Year