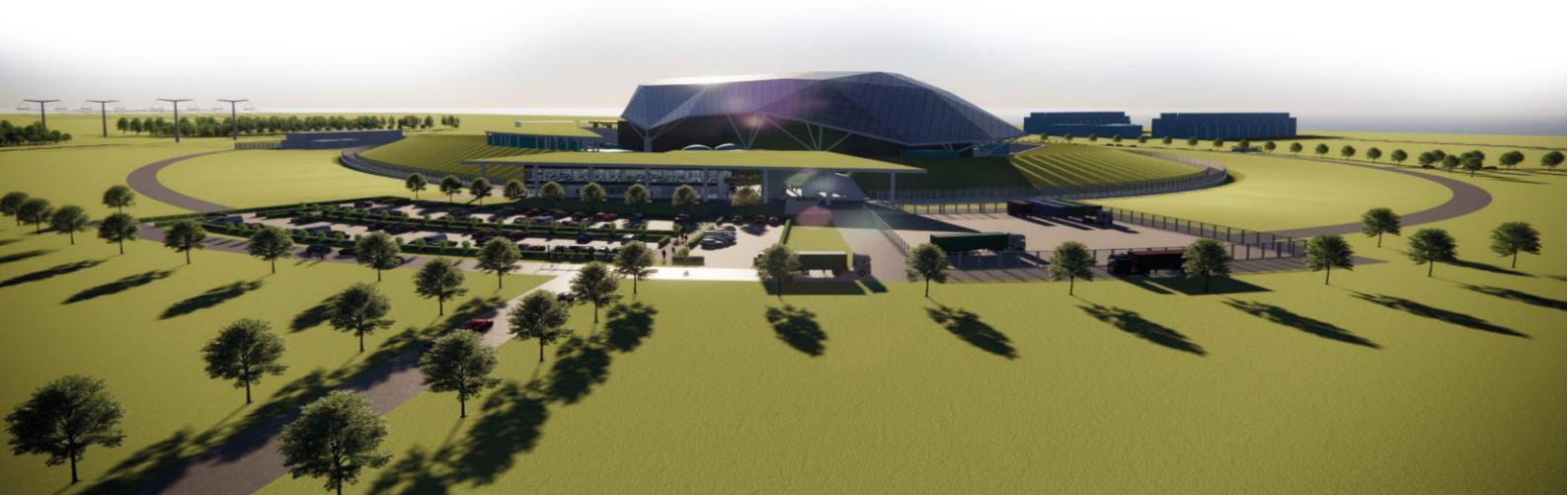
Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs



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 EMIT approach incorporated • Summary of V&V 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 V&V 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 Also minor template/editorial updates for overall E3S Case consistency.

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).

The chapter outlines the arguments and evidence to underpin the top-level claim that suitable E3S design principles and associated methods, approaches, and requirements are established, for the RR SMR to achieve the E3S fundamental objective 'to protect people and the environment from harm'. Their application enables the design and analysis outputs presented throughout the E3S Case to provide a suitable demonstration that risks will be reduced to as low as reasonably practicable (ALARP), apply best available techniques (BAT) and ensure secure by design and safeguards by design.

E3S design principles presented in this chapter cover E3S functions and functional requirements, numerical targets for analysis of the design, the concept of defence in depth (DiD) and its application, application of design requirements to classified SSCs, codes and standards selection commensurate with safety classification, safety analysis techniques, and the E3S categorisation and classification methods. The principles outlined are based on United Kingdom (UK) and international relevant good practice (RGP), such that they provide a suitable framework for the design and analysis of the RR SMR to achieve its E3S objective.

Version 2 of the generic E3S Case is developed in support of the reference design 7 (RD7) design, corresponding to design reference point 1 (DRP 1) for the generic design assessment (GDA). Further arguments and evidence are to be developed to underpin the top-level claim and to achieve the objective of the generic E3S Case, including the refinement of the E3S categorisation and classification process to incorporate relevant learning from its ongoing application across the E3S disciplines.

Contents

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 key principles and associated approaches that provide the framework for the RR SMR to achieve its E3S objectives. The principles and associated approaches are implemented into the RR SMR design development and analysis activities, with compliance against these principles and approaches demonstrated throughout the individual chapters of the E3S Case.

3.0.2 Scope and Maturity

The scope of this chapter covers the general E3S design principles and approaches that govern the design, including design verification of structures, systems, and components (SSCs), for all operating modes and plant states, to ensure the E3S fundamental objective can be met by the RR SMR at all lifecycle stages of design, construction, commissioning, operation, and decommissioning.

The scope of this chapter does not include the detailed policies, standards, requirements, and analysis methods by which the detailed design aspects for each engineering area are evaluated, such as (but not limited to): methods for compliance with structural integrity defect tolerance assessments, shielding assessment methodology for radiation protection, or analysis methodology for assessment of internal and external hazards. This detail is provided within the relevant chapters of the E3S Case.

The 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 2 of the generic E3S Case is based on reference design 7 (RD7), corresponding to design reference point 1 (DRP1) for the generic design assessment (GDA). At RD7/DRP1, the E3S design principles are well established and the approaches to support the RR SMR design and E3S analysis are adopted in the design development process, therefore no significant new information is expected to support this chapter in future revisions of the generic E3S Case to meet its objective.

3.0.3 Claims, Arguments and Evidence Route Map

The overall approach to claims, arguments, evidence (CAE) and the set of fundamental E3S claims to achieve the E3S fundamental objective are described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [1]. The associated top-level chapter claim for E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives & Design Rules for SSCs is:

Claim 3: SSCs are designed and evaluated using suitable and justified approaches and methods, to ensure the E3S fundamental objective 'to protect people and the environment from harm' can be achieved.

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

information, where possible, is also illustrated in the route map, which aligns the anticipated arguments and evidence to future versions of the generic E3S Case (subject to ongoing planning).

A proportionate summary of the arguments and evidence from lower tier information, available at the current design stage, is presented within this chapter. A mapping of the claims to the corresponding sections that summarise the arguments and/or evidence is provided in Appendix A (section 3.5).

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 can be considered as 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 shall be 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 as low as reasonably practicable (ALARP), applying best available techniques (BAT), and ensuring secure by design 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 [3] that provide a framework against which the design is evaluated and developed.

The E3S design principles for the RR SMR have been 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, European Utility Requirements (EUR), Office for Nuclear Regulation (ONR) Safety Assessment Principles (SAPs) and Security Assessment Principles (SyAPs), and Environment Agency (EA) Regulatory Guidance.

3.1.2 E3S Functions

3.1.2.1 Safety Functions

The RR SMR is being designed to achieve the three fundamental safety functions (FSFs) set out in IAEA guidance, at all lifecycle stages. These are defined as:

- Control of reactivity (CoR).
- Control of fuel temperature (CoFT).
- Confinement of radioactive material (CoRM).

An additional 'fourth' FSF has also been defined for RR SMR [3], control of radiation exposure (CoRE).

The FSFs are decomposed into high-level safety functions (HLSFs) in the fault schedule, with safety measures assigned to deliver them. Safety categorised functional requirements are then decomposed onto SSCs that comprise the safety measure, including supporting systems such as control and instrumentation (C&I), electrical power, or heating, ventilation and air conditioning (HVAC).

The evolving fault schedule is linked to the maturing design definition via the requirements management database using the requirements management process, described further in the Deterministic Safety Case Methodologies [4].

HLSFs are assigned a safety category, which is then used to classify the SSC that deliver the HLSFs, in accordance with the categorisation and classification method summarised in Section 3.2 of this chapter.

Safety measures also encompass any required 'human actions' that the operator needs to take to fulfil the HLSF. The systematic assessment and allocation of human actions is performed in conjunction with the Human Factors team, described further in E3S Case Version 2, Tier 1, Chapter 18: Human Factors Engineering [5]. 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 Protection Functions

During engineering design development, SSCs need to be appropriately incorporated into the design of the RR SMR to deliver robust environmental protection. These SSCs are required to perform a specific environmental protection function (EPF), typically guided by relevant EA legislation, standards, and relevant good practice (RGP).

A method for identifying environmental functions under normal radiological operations (including anticipated operational occurrences) has been developed for the design of the RR SMR [6], where the term 'environmental function' is defined as 'a function that is necessary to a facility to prevent detrimental environmental consequences or minimise the impact to people and/or the environment of detrimental environmental consequence'.

The identification of environmental functions and associated environmental measures during the design stage enables future operators to comply with their Radioactive Substances Regulation (RSR) Permit and additional conventional environmental permits.

During the design stage, environmental functions are identified based on the E3S design principles, typically based around categories of containment, treatment and abatement, mitigation, and sampling and monitoring, using RGP, operating experience and professional judgement. Generic 'SMR-level' environmental functions are then identified through attendance of suitably qualified and experienced personnel (SQEP) at engineering and design meetings.

These are recorded as functional requirements that are placed onto the design via the RR SMR requirements management database, with engineering teams (supported by the environment team) responsible for identifying environmental measures to fulfil the functions and the decomposition of requirements onto individual SSCs. Further details on environmental measures and their classification are described in Section 3.2 of this chapter.

3.1.2.3 Security Functions

A methodology for defining security functions has been established for the design of the RR SMR based on UK and international RGP [7]. This includes the definition of physical security functions, which are aligned to the key functions of a physical protection system:

- Deter

- Detect
- Assess
- Minimise insider threat.

Cyber security functions are also defined, including:

- Identify
- Protect
- Detect
- Recover.

These security functions are aligned to the stages of a potential adversary activity, known as an attack lifecycle, described further in [7]. The categorisation of security functions and classification of SSCs is described further in Section 3.2.3.

3.1.2.4 Safeguards Functions

All SSCs required to deliver the safeguards functions are tagged as such in the requirements management database throughout the design phase.

3.1.3 Radiological Protection and 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 ONR SAPs Targets 1 – 9 and align with international guidance and practices (described further in the E3S design principles [3]).

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.

It is noted that irrespective of whether numerical targets have been achieved, doses and risks must be always controlled and reduced to ALARP, which is justified in the design and safety analysis presented throughout the E3S Case, and summarised in E3S Case Version 2, Tier 1, Chapter 24: ALARP Summary [8].

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 10 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 Plant States

The plant states defined for RR SMR are defined as follows:

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

Plant states are aligned to the levels of defence in depth (DiD), described further in Section 3.1.6.

3.1.5 Prevention & Mitigation of Accidents

The RR SMR approach to prevention and mitigation of accidents is through the implementation of DiD, described in Section 3.1.6.

3.1.6 Defence in Depth

The RR SMR is being designed to achieve DiD against postulated initiating events (PIEs) through the provision of consecutive and practicably independent measures over five DiD levels, which would have to fail before harmful effects could be caused to people or to the environment.

The DiD levels are summarised in Table 3.1-2, including alignment to plant states, the objective of each level, the definition of the type of measure associated with the level of DiD, an estimate of the PIE frequency for which that level is generally applicable, and success criteria that measures associated with a level must achieve.

The RR SMR approach for DiD also covers UK RGP for DBC frequent and infrequent faults, defined as:

- Frequent faults: PIEs with an initiating event frequency (IEF) exceeding 1 x 10^{-3}/yr, and unmitigated consequences exceeding BSLs (see Table 3.1-1). A minimum of two practicably independent and diverse measures are provided to deliver the success criteria.
- Infrequent faults: PIEs with an IEF between 1 x 10-3/yr and 1 x 10-5/yr, and unmitigated consequences exceeding BSLs (see Table 3.1-1). A minimum of one measure is provided to deliver the success criteria.

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

For the RR SMR, beyond design basis faults are covered by DECs, defined as:

- DEC-A: PIEs and complex sequences without fuel melt with an IEF <1E-05/year, and unmitigated consequences exceeding BSLs (see Table 3.1-1).
- DEC-B: Severe accident conditions postulated from the inherent hazard potential and from sequences arising from failures of duty, preventive, and protective measures.

Further details and justification for the RR SMR DiD approach, including comparison of plant states with ONR, IAEA, EUR and WENRA, are provided in the E3S design principles [3]. Compliance with the DiD approach is demonstrated through the safety analysis and the plant design.

An important aspect of the implementation of DiD is the provision of multiple, and as far as practicable independent, physical barriers between radioactive material and the environment. The physical barriers for the radioactive material in the reactor core include:

- Fuel matrix and fuel cladding
- Reactor circuit
- Containment and associated systems.

Table 3.1-2: Defence in Depth Levels for RR SMR

DiD Level	Plant State	Plant State ID	Objective	Measure		Postulated Frequency (pa)		Success criteria
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 pa on-site radiation worker <0.1 mSv pa on-site non-radiation worker <0.02 mSv pa 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 / 3	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
3					Frequent fault and failure of the first protective measure	<1E-05	Note 1	
4	Design Extension Conditions (fault conditions)	DEC-A	Control of fault conditions beyond the design basis		Beyond design basis			
4	Design Extension Conditions (accident conditions)	DEC-B	Control of severe accidents	Mitigating				<100mSv 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				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.

3.1.7 Application of General Design Requirements

3.1.7.1 E3S Design Principles

As the design progresses, the E3S design principles [3] are used to guide and inform the ongoing design development process, including through design optioneering and analysis. As part of the systems engineering approach, a comprehensive set of non-functional system requirements (also termed transverse requirements) are also developed from these principles.

The full set of non-functional system requirements derived from the E3S design principles are listed within the requirements management database [9] and applied by the engineering teams to the site, plant, or SSC as part of the requirements definition during the design process [10]. The requirements cover key design principles including, but not limited to:

- Simple and forgiving design:
    - Employment of hierarchy of controls
    - Practical elimination
    - Fail safe design
- Design of Safety Class 1 and 2 SSCs for DBCs:
    - Conservative design to achieve safety functions in most onerous initial conditions and without reliance on other equipment
    - Tolerance to common cause failures
    - Redundancy, including tolerance to Single Failure Criterion for Class 1 SSCs, when in the worst permitted configuration of equipment for outages
    - Segregation of redundant trains
    - Diversity of initiation between safety measures
    - Diversity of onsite essential services
    - Delivery of safety functions without reliance on operator action in the control room within 30 minutes, or outside the control room within 1 hour, unless personnel are already present in the locality of the place where actions are required[1]
    - Delivery of safety functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days
- Best-estimate design of SSCs for DEC-A and DEC-B:
    - Design to deliver safety functions following failures consequential upon the initiating event

[1] E3S design principles allowing operator action within 30 minutes where already present in the locality is aligned to EURs, for example could be applied to moving crane to a safe position following a PIE.

- Design with a supply of on-site essential services diverse from sources claimed for DBC, for sequences where the same essential service is needed for DEC functions and no on-site diversity exists for DBC
- Design to deliver safety functions following accidental aircraft impact
- Delivery of safety functions without reliance on operator action in the control room within 30 minutes, or outside the control room within 1 hour, unless personnel are already present in the locality of the place where actions are required (for DEC-B, without reliance on operation action within 12 hours, ideally 24 hours)
- Delivery of safety functions without reliance on essential services supplied from on-site mobile equipment for 24 hours or from off-site for 7 days, unless personnel are already present in the locality of the place where actions are required
- For DEC-B, tolerance to internal and external hazards

- General design of SSCs:
  - Application of codes and standards commensurate with safety classification
  - Qualification to deliver safety functions within environmental conditions, commensurate with safety classification
  - Design to facilitate Examination, Maintenance, Inspection and Testing (EMIT)
- Design of site and plant layout:
  - Segregation of radiation sources from people
  - Segregation from sources of internal and external hazards
  - Facilitation and control of access and egress, including in response to initiating event
  - Facilitation of construction, installation, commissioning, decommissioning, and demolition.

3.1.7.2 Codes and Standards

SSCs important to nuclear safety shall be designed, manufactured, installed, examined, and inspected using codes, specifications, and standards commensurate with their classification. Codes and standards for nuclear SSCs shall be selected which satisfy the following requirements:

- The codes and standards applied shall reflect the safety categorised functional requirements assigned to the SSCs that deliver a safety function and shall be commensurate with their nuclear safety classification.
- Each code or standard adopted shall be evaluated to determine its applicability, adequacy, and sufficiency.
- Where necessary, codes and standards shall be supplemented or modified as required to achieve a level commensurate with the importance of the relevant safety function(s).

- For Class 1 and Class 2 SSCs, appropriate nuclear industry-specific, national, or international codes and standards shall be adopted where available.

- For Class 3 SSCs, an appropriate nuclear, non-nuclear-specific code or standard shall be applied.

- The combining of different codes and standards for a single aspect of an SSC shall be avoided – where this cannot be avoided, the combining of the codes and standards shall be justified, and their mutual compatibility demonstrated so far as possible.

- Where a single SSC is required to deliver multiple safety functions, and independence between these safety functions cannot be demonstrated, then the codes and standards shall be appropriate to the class of the item (i.e. in accordance with the highest category of safety function to be delivered).

- Where a single SSC is required to deliver multiple safety functions, and independence between these safety functions can be demonstrated to be delivered by the item independently of one another, then separate codes and standards shall be applied appropriate to the parts of the item providing each safety function.

- Whenever different codes and standards are used for different aspects of the same item, the compatibility between these codes and standards shall be demonstrated.

- Where there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, shall be adopted.

- In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, shall be applied to demonstrate that the SSC will perform its safety function(s) to a level commensurate with its classification.

The RR SMR Engineering Management Plan [11] presents the policy for the selection of codes and standards to ensure sound engineering in design. The policy is applicable to the whole RR SMR power station throughout the whole lifecycle of the power station, including design, manufacturing/construction, testing, inspection, maintenance, in service repairs, modification, and decommissioning.

Competent persons are responsible for selecting the codes and standards to be used for their specific discipline, in accordance with the codes and standards policy [12]. The applicable codes and standards are captured as part of the requirements specification for each SSC, including the rationale for selection, justification of their applicability and that they represent RGP. The governance process for selection of codes and standards is defined in the RR SMR gated review process for sentencing the maturity of SSCs through their lifecycle [13].

Selection of codes and standards and their rationale has been undertaken, including:

- Reactor Island C&I codes and standards, documented within [14]

- Electrical power system codes and standards, documented within [15]

- Reactor Island mechanical handling codes and standards, documented within [16]

- Codes and standards for safety class 3 mechanical components, documented within [17]
- Civil and structural codes and standards, documented within [18]

The codes and standards selected for the design of SSCs at RD7/DRP1 are presented in Section 1 of individual chapters across the E3S Case.

3.1.7.3 Examination, Maintenance, Inspection and Testing

EMIT is an integral part of the operation of a nuclear facility in support of equipment reliability for safety, environmental protection, legal compliance, and plant availability. It ensures that both the levels of reliability and availability of all plant SSCs that have a bearing on safety remain in accordance with the assumptions and intent of the design, and that the safety of the plant is not adversely affected after the commencement of operations.

As the design progresses, an overarching fundamental approach has been established for the design of SSCs and their associated EMIT activities [19]. This covers the development of EMIT tasks in accordance RGP and operating experience, such as EUR and Electric Power Research Institute (EPRI) utility requirements, and ensuring the E3S objective is embedded into the design of EMIT to ensure SSCs deliver their E3S requirements through-life, including:

- Application of the E3S design principles in the design development processes for measures and constituent SSCs to enable through-life EMIT, such as: ensuring EMIT can be undertaken at an appropriate frequency to achieve sufficient reliability; undertaking non-intrusive online EMIT where possible, including maintaining availability of higher safety classified measures; and definition of more stringent EMIT procedures proportionate to the E3S classification of the SSC.
- EMIT informed by E3S analysis, including interface with the probabilistic safety analysis (PSA) to derive reliability and maintenance / test interval requirements, and planning of EMIT to optimise plant configuration.
- The E3S classification of equipment used for intrusive online EMIT, for example, a measure comprising three redundant trains that has one train taken offline and put into a testing configuration while the other two trains remain online to deliver their functionality should a demand arise. Given a reduction in redundancy, an increased probability of failure on demand occurs, therefore the equipment required to take the train offline, perform the EMIT, and then return the EMIT to service are important to E3S, and provide a significant role in ensuring E3S. As such, the functionality of the SSC that deliver the EMIT shall be categorised.
- Consideration of human factors integration, including human capabilities and performance, in the design and development of EMIT for SSCs.

EMIT activities are documented in the design definition for each SSC and summarised across the systems engineering chapters of the E3S Case. As EMIT activities are developed through the design process, they are stored within the project's requirements management database with appropriate traceability to the design and the E3S Case, such as the development of technical specifications and Operational Limits and Conditions (OLCs) (to be covered in E3S Case Tier 1, Chapter 16: Operational Limits and Conditions [20]).

3.1.7.4 Verification & Validation

As part of the systems engineering requirements-led approach, the design of the RR SMR undergoes robust verification & validation (V&V) to demonstrate evidence-based compliance with the requirements set, stakeholder needs, and demonstrate design intent, which include E3S requirements as described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [1]. 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.
- Equipment qualification (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.
- Service conditions are the physical conditions prevailing or expected to prevail during the service life of an SSC, such as environmental conditions.

The Rolls-Royce SMR V&V principles are to:

- Progressively build confidence in the Rolls-Royce SMR product as early as possible.
- Prove the design, making use of Rolls-Royce SMR 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 is applied differently depending on the part of the product development lifecycle it is being applied to, including:

- Requirements definition: verification of requirements through technical checking, and validation of requirements that they meet stakeholders needs, described further in [10].
- Design definition:
    - Verification of the design definition to demonstrate that it complies with its requirements, encompassing EQ to demonstrate that SSCs can deliver their E3S functions under the range of service conditions to which they might be exposed to under different operational states, including some fault and accident conditions. The Rolls-Royce SMR 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 & maintenance of the EQ through plant life.

    - Validation of the design definition is generally achieved through the application of design requirements validation and design definition verification define above.

- Implemented solution:

    - Verification of the implemented solution to demonstrate it complies with its design definition, is achieved through manufacturing quality assurance. This shall be conducted in offsite factories and/or onsite as the SSC is being installed/built, described further in E3S Case Version 2, Tier 1, Chapter 14: Plant Construction and Commissioning [21].

    - 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.

Design verification activities carried out to satisfy the E3S requirements of a particular SSC will generate evidence which will be assessed against pre-defined exit criteria, with verification outputs forming the Tier 2 and Tier 3 arguments and evidence required to underpin claims across the E3S Case.

At Version 2 of the generic E3S Case, these outputs primarily comprise design verification strategies for SSCs or specific topics at Tier 2. Verification strategies set out the approach to verify the E3S requirements (as part of the overall requirements set), the sequence in which they should be completed, and the rationale for selection of specific methods. The strategies for each type of E3S requirement may include:

- E3S categorised functional requirements and associated performance requirements:

    - analysis (thermal hydraulic performance) to verify that an SSC can achieve its functional requirement(s) and achieve its success criteria, documented within analysis reports.

    - rig tests to results of the validate performance analysis, documented within specific test reports.

- Non-functional system requirements:

    - inspection of design definition to demonstrate the SSC design achieves an architecture requirement, as documented within system design descriptions (SDDs), for example, segregation of redundant trains to demonstrate tolerance to internal hazards.

Verification strategies will develop into verification compliance reports as the verification evidence is developed and reported in future versions of the E3S Case. These will be supported by detailed verification evidence at Tier 3, such as test and analysis reports and any supporting data (e.g., rig test data, similarity data, analysis results).

The arguments and evidence are summarised in a proportionate manner across the Tier 1 chapters of the E3S Case, with reference to detail in the lower tiers.

Validation outputs for the implemented solution will also be mapped to tiers of the E3S Case, in a similar manner to verification outputs described above, as the validation activities are identified and planned through the ongoing design programme.

Further details of the approach to verification, validation and EQ are presented in the approach to V&V [22].

3.1.8 Safety Analysis

Safety analysis informs the design and provides assurance of the DiD approach outlined in Section 3.1.6. Key analysis techniques and approaches are summarised below, with further detail and outputs of the various analyses described in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [23].

3.1.8.1 Deterministic Safety Analysis

Hazards for the RR SMR are identified using a variety of well-established techniques, such as hazard and operability (HAZOP) studies, failure mode, effects and criticality analysis (FMECA), and human factors (HF) task analysis, from which the hazards are grouped and sentenced into PIEs for assessment in the fault schedule based on frequency of occurrence and unmitigated consequences. This bottom-up approach is complimented by a top-down examination of generic lists of initiating events for pressurised water reactors (PWRs) and how / if they may arise in the RR SMR design.

The outputs of the hazard identification studies are collated in a Hazard Log, which screens the hazards for further assessment, as inputs to the fault schedule for deterministic analysis and the PSA model for probabilistic analysis. The sentencing process is based on the severity of their unmitigated consequences and their frequency of occurrence.

When determining if an initiating event is within the design basis, consequences are calculated on a conservative basis using best available relevant data, and IEFs are calculated on a best estimate basis, except for natural hazards for which a conservative approach is adopted. If a frequency 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, then initiating event is assumed to be within the design basis.

The fault schedule is a focal point of the deterministic safety case and provides an entry point for exploration of the PIEs and the associated safety functions and safety measures. Fault sequences are developed and evaluated in the fault schedule to understand the chronological response for each PIE through each level of DiD to deliver a HLSF, characterising the demand on preventive, protective, and mitigation safety measures in the design.

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. Through specification of safety measures, the fault schedule provides a key interface between the safety analysis and the safety categorised functional requirements placed on the design.

Performance analysis is used to assess fault sequences in the fault schedule to provide high confidence that safety measures can achieve their safety functions. Sequences are modelled using validated computational codes on a best-estimate basis combined with conservative assumptions

(such as application of single failure criterion or failure of non-qualified equipment) and judged against acceptance criteria to provide a suitable safety margin, including radiological dose targets and criteria such as departure from nuclear boiling ratio (DNBR) and peak fuel clad temperature for the reactor.

The plant state 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 generally specified for DBC-2ii and DBC-3i frequent faults than DBC-3ii and DBC-4 and DEC-A infrequent faults and DEC-B accident conditions. Only safety measures that deliver Category A and Category 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 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 OLCs, and performance analysis for DECs will support definition of accident management strategies and emergency procedures.

The RR SMR deterministic safety methodologies [4] and design basis performance analysis methodology [24] provide further detail on the approaches described above.

3.1.8.2 Probabilistic Safety Analysis

PSA studies combine 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 be realised as the RR SMR progresses throughout the plant lifecycle, such as the use of PSA to risk inform EMIT activities or OLCs. At the RD7/DRP1 design stage, PSA has supported development of an overall EMIT strategy for RR SMR, described in Section 3.1.7.3 of this chapter.

Further details on the PSA strategy, approach, and maturity at this stage of design are presented in the PSA development strategy [25].

3.1.8.3 Severe Accident Analysis

Severe accidents have the potential to involve phenomena which pose both immediate and delayed threats to the FSF of CoRM (see Section 3.1.2), resulting in major consequences to the public and environment. Severe accident analysis (SAA) is undertaken for the RR SMR design to assess a representative range of postulated severe accident progression behaviours, with the aim to avoid, so far as is reasonably practicable (SFAIRP), the loss of CoRM in the short term, and to preserve, SFAIRP, the CoRM in the long term.

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, severe accident SSCs are modelled to demonstrate containment conditions in DEC-B severe accidents can achieve relevant acceptance criteria, such as containment integrity. Safety categorised functional requirements are defined and severe accident measures, identified as DiD level 4 in the fault schedule, are categorised in accordance with the methodology outlined in Section 3.2.

The aims of the SAA as the design progresses are to support demonstration of 'practical elimination' of large or early releases through the design, or that design measures can mitigate the accident progression and radiological consequences. It also supports the demonstration that there are no 'cliff-edge' effects in the safety analysis through the levels of DiD and supports EQ through definition of the safe operating envelope under severe accident conditions.

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.

Other SAA applications will be realised as the RR SMR progresses throughout the plant lifecycle, such as development of severe accident management strategies, guidelines and procedures, and offsite emergency planning activities.

Further details of the SAA strategy, approach, and maturity at this stage of design are presented in the severe accident management strategy [26].

3.1.8.4 Internal Hazards

In addition to plant faults, the design of the RR SMR considers evaluation of internal hazards, i.e., hazards arising from within the bounds of the power station that are considered as PIEs that could challenge the delivery of safety functions. Where reasonably practicable, the aim of the RR SMR is to ensure an inherently safe design, or where this is not achievable, to demonstrate tolerance to hazards to ensure a safe state can be reached and the risk is reduced to ALARP. E3S design principles and requirements relevant to internal hazards have been identified to inform the layout during the concept design stage, with internal hazards specialist support provided to layout and design teams, to eliminate or minimise the impact of internal hazards.

The assessment and protection measures for internal hazards for RR SMR takes cognisance of RGP and guidance from the ONR and other international nuclear regulatory bodies. The internal hazards approach for RR SMR is largely built upon the concept of segregation of SSCs within the design through physical distance (separation) or physical barriers to ensure that individual losses of equipment can be tolerated due to redundant equipment remaining available. The role of operators will also be considered and the need for access and egress, as well as impacts on barriers and other SSC.

The identification of internal hazards includes a consideration of the initial conditions, the magnitude and the likelihood of the hazards, the locations of the sources of the hazards, the resulting environmental conditions, and the possible impacts on SSCs important to safety or on other SSCs. Assessment considers whether a PIE occurs due to a hazard, and whether the hazard can damage the safety measures for that PIE.

The assessment process also considers potential hazard combinations, including consequential hazards whereby a primary hazard initiates a secondary hazard that becomes the PIE, correlated hazards whereby more than one hazard is initiated by the same cause, independent hazards whereby there is no causal relationships between the combinations, and external-internal hazard combinations. Screening is applied to aid rationalisation of combinations to ensure the focus of assessment remains on those combinations that pose a foreseeable threat to SSCs and barrier.

The internal hazards sequences are included in the fault schedule, with deterministic assessment used to define hazard protection requirements, such as divisional barriers or pipe whip constraints. Safety categorised functional requirements are defined, and hazard protection measures are classified in accordance with the methodology outlined in Section 3.2, which are substantiated through the design and V&V process.

Further details on the internal hazards assessment strategy and approach are presented in the internal hazard strategy [27].

3.1.8.5 External Hazards

In addition to plant faults, the RR SMR evaluates external hazards, including combinations of external hazards, in the context of nuclear safety, i.e., hazards arising from outside the bounds of the power station that are considered as PIEs that could challenge the delivery of safety functions. An external hazard is a natural or man-made hazard which originates externally to both the site and its processes.

External hazard studies demonstrate that risks are reduced ALARP through the derivation of appropriately conservative hazard parameters from RGP and incorporating those values into the RR SMR design. The effects of climate change over a 100-year period following initial deployment will be considered, covering the design operational life of the RR SMR, potential lifetime extension and estimated decommissioning period.

The external hazards associated with RR SMR are defined in E3S Case Version 2, Tier 1, Chapter 2: Generic Site Envelope [28], which have been determined using techniques that are RGP and are supported by both national and international guidance. External combined hazards and hazards associated with space weather are also characterised.

The hazard frequencies for determining the magnitudes of the events have been developed from the RR SMR E3S design principles [3]. For hazards that can be characterised with non-discrete frequency of exceedance hazard curves, the design basis is set based on:

- Naturally occurring external events with frequency ≥1E-04 per year, as calculated on a conservative basis.
- Manufactured external hazards and internal hazard events with frequency ≥1E-05 per year, as calculated on a best estimate basis.

The design should ensure normal operation is available following the less severe and more probable hazard operating basis events. No SSC should be impaired by the repeated occurrence of operating basis events. For discrete hazards, the design basis is set in accordance with Table 3.1-2.

External hazard studies are used to inform the design, including dedicated SSCs where reasonably practicable to prevent escalation of postulated hazards to initiating events and to prevent damage to classified SSCs that may be claimed against any induced initiating event, for example the hazard shield.

3.1.8.6 Conventional Safety Analysis

Conventional safety requirements are derived to inform the design, based on regulation, legislation, and directive compliance. The design for conventional safety process [29] adopted by the RR SMR outlines the overarching approach, with conventional safety legislation and regulation fully integrated within our design management systems, processes, and procedures, rather than undertaken as auxiliary activities, as more commonly the practice. Building on this foundation, RR SMR aims to assure emergent requirements and relevant good practices are also captured and will undertake assessments at pertinent points to secure additional safety benefits appropriately.

3.2 Categorisation and Classification

3.2.1 Safety Categorisation and Classification

DiD is achieved through the provision of multiple practicably independent 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 standards and RGP to which SSCs are designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected, with more stringent standards required for higher classified SSCs. The RR SMR codes and standards are described further in Section 3.1.7.2.

The RR SMR safety categorisation and classification method, justified in [30], 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 Measures over the Levels of Defence in Depth

Safety measure and its role in delivering Defence in Depth			Undefended Dose Consequence	>100 mSv *off-site*	10 – 100 mSv *off-site*	1 – 10 mSv *off-site*	0.1 – 1 mSv *off-site*	0.01 - 0.1 mSv *off-site*
				>500 mSv *on-site*	200-500 mSv *on-site*	20-200 mSv *on-site*	1-20 mSv *on-site*	0.1-1 mSv *on-site*
Duty	Number of measures available to deliver Cat A or Cat B functionality in subsequent levels of DiD	0		A	A	A	A	B
		1	when that subsequent functionality is Cat A	B	B	B	B	-
			when that subsequent functionality is Cat B	C	C	C	C	C
		2		C	C	C	-	-
Preventive	Number of preventive measures needed to reduce the demand for protective measure functionality in subsequent levels of DiD	0		C	C	C	C	C
		1	when reducing demand to nil or Cat C	A	A	A	A	B
			when reducing demand from two measures to a single measure delivering Cat A functionality	B	B	B	-	-
		2		A+B	A+B	A+B	-	-
Protective	Postulated protective measure demand frequency (per year)	>1E-01		A+B	A+B	A+B	A	B
		1E-01 – 1E-02		A+B	A+B	A	B	C
		1E-02 – 1E-03		A+B	A	A	B	-
		1E-03 – 1E-04	when reasonably practicable to provide a single protective measure only	A	A	B	-	-
			when reasonably practicable to provide two protective measures	A+B	A+B	B+C	-	-
		1E-04 – 1E-05	when reasonably practicable to provide a single protective measure only	A	C	C	-	-
			when reasonably practicable to provide two protective measures	A+B	C+C	C+C	-	-
		1E-05 – 1E-06		C	C	-	-	-
		1E-06 – 1E-07		C	-	-	-	-
		<1E-07		-	-	-	-	-
Mitigating				C	-	-	-	-

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 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.

- 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 outputs of the application of the categorisation and classification method for each SSC is presented throughout the engineering chapters of the E3S Case.

3.2.2 Environmental Categorisation and Classification

As described in Section 3.1.2.2, environmental measures are identified to fulfil SMR-level environmental functions that are captured as requirements on the design. These environmental measures are classified to determine their importance with respect to environmental protection.

An environmental classification does not dictate any additional requirements on that SSC, e.g., 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 environmental 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 requirements management database against the relevant environmental function but are not assigned a classification. Detail of the administrative measures will be developed as part of human factors design, including allocation of function to operators.

The environmental classification method [6] describes how environmental functions and associated environmental measures to fulfil them are identified using existing tools for engineering design such as hazard identification studies and application of BAT methodologies.

Engineering teams, in conjunction with the environment team, are responsible for identifying environmental measures to fulfil the functions and the decomposition of requirements onto individual SSCs. The SSCs that form the environmental measure will be identified within design definition information using an 'environmentally significant' attribute.

The RR SMR will continue to be optimised as part of the ongoing design development, this is likely to result in identification of further derivation of environmental functions and measures.

3.2.3 Security Categorisation and Classification

As described in Section 3.1.2, security functions are captured for the RR SMR design and aligned to. to the stages of a potential adversary activity. 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 [7]. Security analyses are undertaken to identify the consequence level, including vital area identification and categorisation (VAI&C), categorisation for theft (CfT), and cyber security risk assessment (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 [31].

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.

- 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.

3.2.4 Safeguards Categorisation and Classification

All SSCs required to deliver the safeguards functions are tagged as such in the requirements management database 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 [32] 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 Version 2, Tier 1, Chapter 2: Generic Site Characteristics [28]. 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.

3.2.6 Summary of SSC Classification

The E3S and seismic categorisation and classification for each SSC is presented throughout E3S Case Version 2, Tier 1, Chapters 4 to 11. A list of the main SSCs important to E3S, together with their E3S and seismic classification at RD7/DRP1, are summarised in Table 3.6-1 in Appendix B (section 3.6).

3.3 Conclusions

3.3.1 ALARP, BAT, Secure by Design, Safeguards by Design

The principles and approaches described in this chapter are being applied to the ongoing development of the design, analysis, and verification of SSCs, to ensure the E3S fundamental objective can be met by the RR SMR at all lifecycle stages. Their application enables the design and analysis outputs presented throughout the E3S Case to provide a suitable demonstration that risks are and/or will be reduced to ALARP, apply BAT and ensure secure by design and safeguards by design.

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

None identified in this revision.

3.3.3 Conclusions and Forward Look

The generic E3S Case objective at Version 2 is ‘to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design’ [1]. This confidence is built through development and underpinning of top-level claims across each chapter of the E3S Case, through supporting arguments and evidence. The top-level claim for chapter 3 is 'SSCs are designed and evaluated using suitable and justified approaches and methods, to ensure the E3S fundamental objective 'to protect people and the environment from harm' can be achieved’.

The arguments and evidence presented to meet the generic E3S Case objective at Version 2 primarily include the E3S design principles and a description of the adopted approaches to achieve the principles. Further detail of specific analysis methodologies is described within the relevant analysis chapters of the E3S Case.

The principles and approaches presented in this chapter are based on UK and international RGP, such that they provide a suitable framework for the design and analysis of the RR SMR. They cover E3S functions and functional requirements, numerical targets for analysis of the design, the concept of DiD and its application, application of design requirements to classified SSCs, codes and standards selection commensurate with safety classification, safety analysis techniques, and the E3S categorisation and classification methods.

Further arguments and evidence will be developed in line with the E3S Case Route Map [2] and reported in future revisions of the generic E3S Case, which will further build confidence that the RR SMR can deliver its fundamental E3S objective. This broadly includes refinement of the E3S categorisation and classification process to incorporate relevant learning from its application across the Environment, Security and Safeguards disciplines, and further assignment of E3S and seismic classifications to SSCs important to E3S.

3.4 References

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

[2] Rolls-Royce SMR Limited, SMR0002155 Issue 3, E3S Case Route Map, November 2023.

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

[4] Rolls-Royce SMR Limited, SMR0000531/002, “Rolls-Royce SMR Deterministic Safety Case - Methodologies,” January 2024.

[5] Rolls-Royce SMR Limited, SMR0004520 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, TIer 1, Chapter 18: Human Factors Engineering,” May 2024.

[6] Rolls-Royce SMR Limited, SMR0005548 Issue 1, Identification of Environment Functions and Environmental Measures, July 2023.

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

[8] Rolls-Royce SMR Limited, SMR0004487 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 24: ALARP Summary,” May 2024.

[9] SMR DOORS Database, Transverse Module, /00_Small Modular Reactor/90 - Cross Cutting Concerns/Transverse Requirements, Module Baseline 1.6.

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

[11] Rolls-Royce SMR Limited, SMR0000520/003, “Engineering Management Plan for Rolls-Royce SMR,” October 2022.

[12] Rolls-Royce SMR Limited, SMR0003023/001, “Rolls-Royce Small Modular Reactor Codes and Standards,” October 2022.

[13] Rolls-Royce SMR Limited, C3.2.1-2, “DR Process Guidance,” 2022.

[14] Rolls-Royce SMR Limited, SMR0004273 Issue 2, Reactor Island C&I Codes and Standards Selection Report, June 2023.

[15] Rolls-Royce SMR Limited, SMR0006160 Issue 1, Electrical Power System Codes and Standards, July 2023.

[16] Rolls-Royce SMR Limited, SMR0008184 Issue 1, Reactor Island Mechanical Handling Codes & Standards, October 2023.

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

[18] Rolls-Royce SMR Limited, SMR0006030 Issue 1, Civil and Structural Codes and Standards Policy, June 2023.

[19] Rolls-Royce SMR Limited, SMR0009111 Issue 1, RR SMR EMIT Strategy, December 2023.

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

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

[22] Rolls-Royce SMR Limited, SMR0008444 Issue 1, Rolls-Royce SMR Approach to Verification and Validation, December 2023.

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

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

[25] Rolls-Royce SMR Limited, SMR0004735 Issue 2, Probabilistic Safety Assessment Development Strategy, January 2024.

[26] Rolls-Royce SMR Limited, SMR0005258 Issue 1, Severe Accident Management Strategy, May 2023.

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

[28] Rolls-Royce SMR Limited, SMR0004542 Issue 3, "Environment,Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 2: Generic Site Characteristics," May 2024.

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

[30] Rolls-Royce SMR Limited, SMR0006518 Issue 1, "RR SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method," July 2023.

[31] Office for Nuclear Regulation, "Security Assessment Principles for the Civil Nuclear Industry - Classified Annexes," March 2022.

[32] Rolls-Royce SMR Limited, SMR0001391 Issue 2, "Rolls-Royce Small Modular Reactor Seismic Performance Classification Method," October 2022.

3.5 Appendix A: Claims, Arguments, Evidence

Table 3.5-1 provides a mapping of the claims to the corresponding sections of the chapter that summarise the arguments and/or evidence. The full decomposition of claims and link to underpinning Tier 2 and Tier 3 information containing the detailed arguments and evidence is presented in the E3S Case Route Map [2]. The route map includes the trajectory of Tier 2 and Tier 3 information as the generic E3S Case develops, which will be incorporated into Tier 1 chapters as it becomes available and in line with generic E3S Case issues described in [1].

Table 3.5-1: Mapping of Claims to Chapter Sections

Claim	**Section of Chapter 3 containing Arguments / Evidence summary**
The E3S fundamental objective is achieved through application of E3S design principles, which are derived from UK and international Relevant Good Practice	3.1.1.2
Fundamental safety functions are defined and can be fulfilled by SSCs	3.1.2
E3S functions are categorised, and the SSCs that deliver them are classified, using suitable and justified methods	3.2 Table 3.6-1
Public and worker dose and risk is evaluated against suitable criteria to support demonstration of ALARP	3.1.3
The concept of Defence in Depth to prevent, protect and mitigate failures across all plant states is adopted in the design	3.1.6
A comprehensive set of non-functional system requirements are developed from the E3S design principles, and applied to the site, plant, or SSC	3.1.7.1
Codes and standards selected for design, manufacturing / construction testing, inspection, maintenance, in-service repairs, modification, and decommissioning of SSCs are commensurate with their safety classification, and appropriately justified when applied to SSCs	3.1.7.2
Conservative analysis methods are used to inform and evaluate the design and demonstrate suitable margins to avoid cliff-edge effects	3.1.8
An overarching approach to EMIT is defined to ensure SSCs can deliver E3S requirements through life	3.1.7.3
A robust approach to verification and validation is adopted to demonstrate SSCs achieve their specified E3S requirements through the lifecycle	3.1.7.4

3.6 Appendix B: Summary of SSC Classification

Table 3.6-1 is populated with classifications that are assigned and documented within SDDs as at RD7/DRP1. As SSC classifications continue to be confirmed and assigned through the design process, this table will continue to be populated in future versions of the generic E3S Case [1]. Note that a system, structure, or component may attract different classifications to different parts of it, and that this table presents the highest or majority classification for each SSC.

Table 3.6-1: Summary of SSC Classification

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
JAC10	Reactor vessel internals	1				SPC1	
JAC20	Fuel assemblies	1				SPC1	
JAC30	Neutron sources	1				SPC1	
JDE	Control rods	1				SPC1	
JAA	Reactor vessel	VHR				SPC1	
JAB	Reactor vessel closure head	VHR				SPC1	
JAB10	Reactor pressure vessel closure assembly	VHR				SPC1	
JAB20	Control rod drive mechanism cooling system						
JAB30	Integrated head package lifting assembly	1				SPC1	
JAB40	Integrated head package structure	1				SPC1	
JAH	Reactor pressure vessel insulation						
JE	Reactor coolant system	VHR					
JEA	Steam generation system	VHR					
JEB	Reactor coolant pump system	VHR					
JEC	Reactor coolant pipework system	1					
JEF	Reactor coolant pressurising system	VHR					
JEG	Reactor coolant pressure relief system	1					

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
JNA	Cold shutdown cooling system	2				SPC1	
KB	Chemical and volume control system	3					
KBA	Level and volume control system	3					
KBD	Chemistry control system	3					
KBE	Coolant purification system	1					
JD01	Scram safety measure	1				SPC1	
JD02	Alternative shutdown function safety measure	2				SPC1	
JDK	Emergency boron injection system	2				SPC1	
JM	Reactor plant containment systems						
JMA	Containment vessel structure	1				SPC1	
JM01	In-vessel retention safety measure	3					
JMB	Core melt stabilisation system						
JMD	Containment penetration for fuel transfer						
JME	Equipment transfer airlock						
JMF	Personnel airlock						
JMK	Containment mechanical penetrations						
JML	Containment cable penetrations						
JMM	Containment leak monitoring and collection						
JMN	Containment spray						
JMR	Containment venting and filtering						
JMS	Hydrogen mixing						
JMT	Hydrogen reduction	2				SPC1	
JMU	Hydrogen monitoring						
JN	Reactor heat removal systems						

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
JNM	Reactor vessel cavity injection system	1				SPC1	
JN01	Emergency core cooling safety measure	1				SPC1	
JNF	Automatic depressurisation system	1				SPC1	
JNG	Low pressure injection system	1				SPC1	
JN02	Passive decay heat removal safety measure	2				SPC1	
JNB	Passive steam condensing system	1				SPC1	
JND	High pressure injection system	2				SPC1	
JNK	Local ultimate heat sink system	1				SPC1	
JN03	Shut down decay heat removal system						
FAN	Emergency heat removal system for coolant used for storage of spent fuel assemblies						
FCF	Airlock system for fuel assemblies /reactor internals between rooms						
KAX	Safety measure coolant supply subsystem						
KH	Nuclear heat tracing systems						
LJ	Emergency feedwater supply system	3					
JRA	Reactor protection system	2				SPC1	
JQA	Diverse protection system	1				SPC1	
JRQ	Accident management system	1				SPC1	
JSA	Reactor plant control system	3					
JSS	Reactor monitoring system						
MY	Turbine island control and protection system	3					
LY	Feedwater, steam and condensate control and protection system	3					

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
PY	Cooling water island control and protection system	3					
KY	Radioactive waste management system C&I	3					
FY	Fuel route C&I	3					
A	Grid transmission system						
AC	Interface to grid transmission system	3					
B	Electrical power system						
BB	High Voltage (HV) Main Alternating Current (AC) supply system	3					
BC	HV Main AC standby supply system	3					
BD	HV Essential AC standby supply system	2				SPC1	
BF	Low Voltage (LV) Main AC supply system for process equipment	3					
BG	LV Main AC supply system for non-process equipment	3					
BK	LV Essential AC standby supply system	2				SPC1	
BL	LV Essential AC alternate supply system						
BM	LV Uninterruptible AC supply system	2				SPC1	
BP	LV Uninterruptible Direct Current (DC) supply system	3					
BQ	LV Uninterruptible DC supply system safety services	1				SPC1	
MS	Generator transmission main connection						
XF	Earthing and lightning protection system	1				SPC1	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
XQ	Lighting systems						
F	Handling of nuclear equipment	1					
FA	Internal fuel storage						
FAA	New fuel receipt and inspection area						
FAB	Storage of spent/irradiated fuel assemblies and other radioactive parts system [FAB]	1					
FAE	Refuelling cavity	1					
FAF	Refuelling pool	1					
FAK	Spent fuel cooling system	2					
FAL	Spent fuel coolant purification system	3					
FAM	System for removal of surface contaminants on components in fuel assembly storage						
FAT	Coolant supply system	3					
FB	Handling of fuel assemblies and other reactor core internals						
FBC	Cleaning system for fuel assemblies (also includes reflector assemblies)	3					
FCJ	System for conveyance of fuel assemblies/internals within reactor area						
FCK	System for conveyance of fuel assemblies/internals between reactor and storage areas	1				SPC1	
FCL	System for conveyance of fuel assemblies/internals within storage area						
FD	External storage of spent fuel						
KA	Nuclear auxiliary systems						
KJ	Nuclear chilled water systems	1					

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
KL	HVAC systems in controlled areas and exclusion areas	1					
KU	Reactor coolant sampling system						
PA	Main cooling water system	3					
PB	Essential service water system	2					
PE	Auxiliary cooling and make-up system	3					
PG	Turbine island closed cooling water system	3					
PU	Common systems for the cooling water systems	3					
G	Water supply disposal and treatment system						
GA	Water supply System						
XBF	Space heating system in structures for handling of nuclear equipment						
XBJ	Space heating system in structures for nuclear heat generation						
XBK	Space heating system in structures for nuclear auxiliary systems						
XG	Fire extinguishing system	3					
XK	Chilled water system						
XM	Mechanical Handling System						
XV	Rainwater systems						
U	Structures and areas for systems inside of the power plant process						
U01	Reactor island structures and areas						
UW	Structures for common systems						
UWA	Seismic isolation system	1				SPC1	

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
UWB	Foundation and basemat	1				SPC1	
UWC	Retaining wall	1				SPC1	
UWD	Hazard shield	1				SPC1	
UF	Structures for the handling of nuclear equipment						
UFA	Structure for internal storage of fuel assemblies (if separate from reactor building [UJA]	1				SPC1	
UJ	Structures for reactor plant						
UJA	Reactor building interior	1				SPC1	
UK	Structures for reactor auxiliary systems						
UKA	Reactor auxiliary building						
UKB	Reactor ancillary building						
UPJ	Structures for cooling towers (auxiliary and secondary processes)	2				SPC1	
UPJ10	ESWS cooling tower 1						
UPJ20	ESWS cooling tower 2						
UBM	Structures for power generation for safety services	2				SPC1	
UBM01	Backup generation 1 and fuel store						
UBM02	Backup generation 2 and fuel store						
L	Steam water condensate system						
LA	Feedwater system	3					
LB	Steam system	3					
LC	Condensate system	3					
LD	Condensate polishing system						
LX	Fluid supply systems for control and protection systems						

RDS-PP®	SSC	Classification					Principal Code(s)
		Safety	Environment	Security	Safeguards	Seismic	
M	Main turbine generator system						
MA	Steam turbine system	3					
MK	Generator system	3					
MU	Common systems of the main turbine generator system	3					
KM	Solid radioactive waste processing systems						
KN	Liquid radioactive effluent processing system						
KNF	Processing and treatment system for liquid radioactive effluent	3					
KP	Gaseous radioactive effluent processing systems						
KT	Reactor island collection and drainage system						

3.7 Abbreviations

AC	Alternating Current
ALARP	As Low As Reasonably Practicable
BAT	Best Available Techniques
BS	British Standard
BSL	Basic Safety Level
BSO	Basic Safety Objective
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CDF	Core Damage Frequency
CfT	Categorisation for Theft
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRE	Control of Radiation Exposure
CoRM	Confinement of Radioactive Material
CSRA	Cyber Security Risk Assessment
DBC	Design Basic Condition
DBE	Design Basis Earthquake
DC	Direct Current
DEC	Design Extension Condition
DiD	Defence in Depth
DNBR	Departure from Nuclear Boiling Ratio
E3S	Environment, Safety, Security, and Safeguards
EA	Environment Agency
EMIT	Examination, Maintenance, Inspection and Testing
EPF	Environmental Protection Function
EPRI	Electric Power Research Institute
EQ	Equipment Qualification
EUR	European Utility Requirements

FMECA	Failure Mode, Effects and Criticality Analysis
FSF	Fundamental Safety Function
HAZOP	Hazard and Operability
HF	Human Factors
HLSF	High-Level Safety Function
HV	High Voltage
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IEF	Initiating Event Frequency
LRF	Large Release Frequency
LV	Low Voltage
OBE	Operating Basis Earthquake
OLC	Operational Limit and Condition
ONR	Office for Nuclear Regulation
PDS	Plant Damage State
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
RGP	Relevant Good Practice
RR SMR	Rolls-Royce Small Modular Reactor
RSR	Radioactive Substances Regulation
SAA	Severe Accident Analysis
SAPs	Safety Assessment Principles
SDD	System Design Description
SFAIRP	So Far As Is Reasonably Practicable
SPC	Seismic Performance Class
SQEP	Suitably Qualified and Experienced Personnel
SSC	Structure, System and Component

UK	United Kingdom
V&V	Verification & Validation
VAI&C	Vital Area Identification And Categorisation
WENRA	Western European Nuclear Regulators' Association