Partner Document Number	Partner Document Issue /Revision	Retention category:
n/a	n/a	A

Title

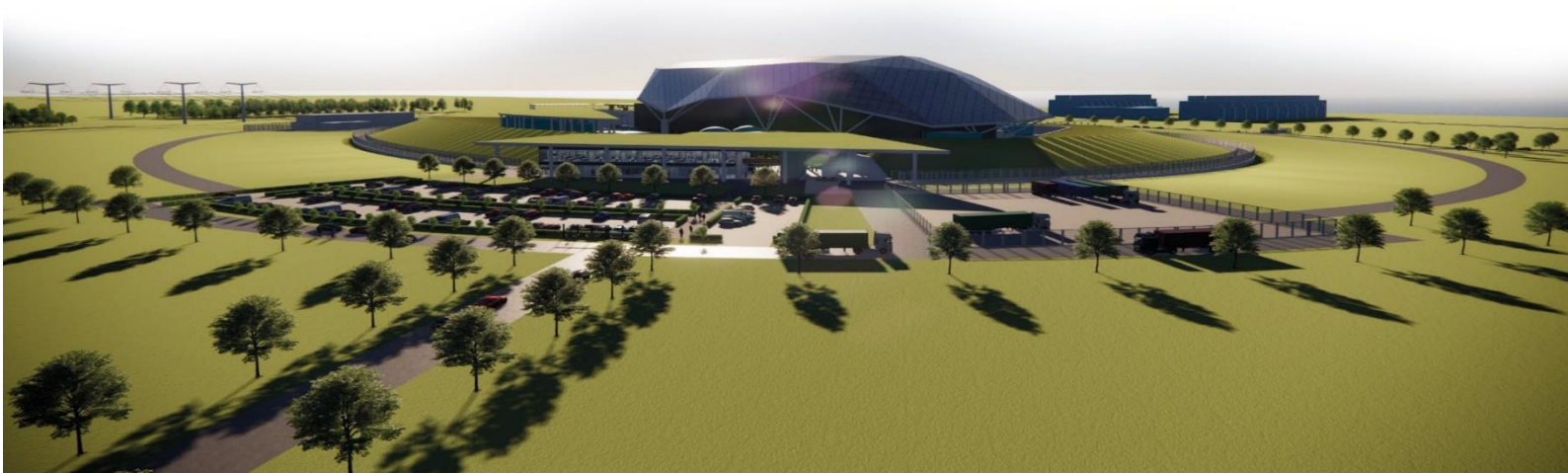
E3S Case Chapter 3: E3S Objectives & Design Rules for SSCs

Executive Summary

Chapter 3 of the Environment, Safety, Security, and Safeguards (E3S) Case presents the E3S objectives and design rules for the Systems, Structures and Components (SSCs) of the Rolls-Royce Small Modular Reactor (RR SMR). The chapter outlines the arguments and evidence available at the Preliminary Concept Definition (PCD) design stage to underpin the high-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'.

E3S design principles presented in this report 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 Systems, Structures and Components (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.

The E3S Design Principles are well established and have informed the PCD design, noting further evidence is to be developed to underpin the overall Claim, including approaches to derive and categorise environmental, security and safeguards functions, specify a comprehensive set of non-function system requirements for the design based on the principles, and further development of codes and standards.



Contents

Tables

3.0 Introduction

3.0.1 Introduction to Chapter

Chapter 3 of the Rolls-Royce Small Modular Reactor (RR SMR) Environment, Safety, Security & Safeguards (E3S) Case forms part of the Pre-Construction Safety Report (PCSR), and is a supporting reference to the Generic Environment Report (GER) and Generic Security Report (GSR), as defined in E3S Case Chapter 1: Introduction, Reference [1].

Chapter 3 presents the key principles and associated methods, approaches, and requirements 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 demonstrated throughout the individual chapters of the E3S Case.

3.0.2 Scope

The scope of this chapter covers the general E3S design principles, approaches, methods, and requirements that govern the design and analysis of Structures, Systems and Components (SSCs), for all operating modes and plant states, to ensure the E3S 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. Such detail is provided in the individual engineering and analysis chapters of the E3S Case.

The design and operation of site factories, and siting aspects and land quality management that are not set by the generic design, are all out of scope.

Design/Programme Maturity

The E3S design principles are well established and many of the approaches to support the RR SMR design and E3S analysis are adopted in the design development process at the Preliminary Concept Definition (PCD) design stage. Aspects that are still in development at PCD are highlighted within the report, including derivation of environmental, security and safeguards functions and the methodology for their subsequent categorisation and classification, formalisation of non-functional system requirements based on the E3S design principles, and further development of a complete set of codes and standards for each engineering discipline.

3.0.3 Claims, Arguments, Evidence Route Map

The Chapter level Claim for E3S Case Chapter 3: E3S Objectives & Design Rules for SSCs is:

Claim 3: Suitable E3S design principles and associated methods, approaches, and requirements are established for the RR SMR to achieve the E3S fundamental objective

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

The complete suite of evidence to underpin the Claims in the E3S Case will be generated through the RR SMR design and E3S Case programme and documented in the Claims, Arguments, Evidence (CAE) Route Map, Reference [2], described further in E3S Case Chapter 1: Introduction, Reference [1].

3.1 General E3S Design Basis

3.1.1 E3S Objectives

Fundamental Objective

The fundamental E3S 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).

E3S Design Principles

To achieve the E3S fundamental objective, a hierarchical decomposition of a set of E3S Design Principles have been established, presented in Reference [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

Safety Functions

The RR SMR is being designed to achieve the three Fundamental Safety Functions (FSFs), at all lifecycle stages. These are defined as:

1. Control of Reactivity (CoR)

2. Control of Fuel Temperature (CoFT)

3. Confinement of Radioactive Material (CoRM)

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 traceability from the Fault Schedule through to the design definition is managed within Dynamic Object Orientated Requirements System (DOORS) through the

requirements management process, described further in the Deterministic Safety Case Methodologies, Reference [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 3.2.1 of this report.

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 Chapter 18: Human Factors Engineering, Reference [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.

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 legislation, standards, and RGP.

EPFs and SSCs as Environmental Protection Measures (EPMs) will be identified through environmental assessments in the GER, with requirements placed onto the SSCs delivering the EPMs that will be managed via the RR SMR requirements management process (within DOORS).

The development of the methodology for identifying EPFs and EPMs is ongoing and will be reported in a future revision of the E3S Case in line with the CAE Route Map.

Security and Safeguards Functions

The development of the methodology for identifying Security and Safeguards functions for the RR SMR is ongoing and will be reported in a future revision of the E3S Case in line with the CAE Route Map.

3.1.3 Radiological Protection & 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 the against 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, Reference [3]).

Two numerical target values for dose/risk are defined:

1. A dose/risk target that shall be achieved by the design, defined as the boundary between tolerable and unacceptable, i.e. the BSL

2. 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 Chapter 24: ALARP Summary, Reference [6].

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	20mSv	1mSv
Annual effective dose for any site worker that does not work with ionising radiation		2mSv	0.1mSv
Average annual effective dose to defined groups of employees working with ionising radiation		10mSv	0.5mSv
Annual effective dose for any person off the site		1mSv	0.02mSv
Hourly dose rate to non-human species		N/A	40µGy
Effective dose received by any person on-site arising from any single fault sequence within the design basis	Fault Conditions	20mSv for IEF > 1E-03 pa 200mSv for 1E-03 < IEF < 1E-04 pa 500mSv for 1E-04 < IEF < 1E-05 pa	0.1mSv
Effective dose received by any person off-site arising from any single fault sequence within the design basis		1mSv for IEF > 1E-03 pa 10mSv for 1E-03 < IEF < 1E-04 pa 10mSv for 1E-04 < IEF < 1E-05 pa	0.01mSv

Metric	Plant State	Shall be lower than (BSL)	Should be lower than (BSO)
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: 2-20mSv 20-200mSv 200-2000mSv >2000mSv		 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: 0.1-1mSv 1-10mSv 10-100mSv 100-1000mSv >1000mSv		 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:

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

1. 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

2. 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:

1. DEC-A: PIEs and complex sequences without fuel melt with an IEF >1 x 10^{-8}/yr, and unmitigated consequences exceeding BSLs (Table 3.1-1)

2. 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, Reference [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:

1. Fuel matrix and fuel cladding

2. Reactor circuit

3. Containment and associated systems

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

<table>
<tr><th>DiD Level</th><th>Plant State</th><th>Plant State ID</th><th>Objective</th><th colspan="2">Measure</th><th colspan="2">Postulated Frequency (pa)</th><th>Success criteria</th></tr>
<tr><td>1</td><td>Design Basis Conditions (normal operation: desired conditions)</td><td>DBC-1</td><td>Prevention of abnormal operation and failures by design</td><td rowspan="2">Duty</td><td>Desired operating conditions</td><td rowspan="4">>1E-02</td><td></td><td><1mSv pa on-site radiation worker
<0.1mSv pa on-site non-radiation worker
<0.02mSv pa off-site
No physical barriers breached where reasonably practicable</td></tr>
<tr><td rowspan="2">2</td><td>Design Basis Conditions (normal operation: abnormal conditions)</td><td>DBC-2i</td><td>Prevention of fault conditions and control of abnormal operation</td><td>Minor deviation from desired operating conditions</td><td rowspan="3">Note 1</td></tr>
<tr><td rowspan="4">Design Basis Conditions (fault conditions)</td><td>DBC-2ii</td><td rowspan="4">Control of fault conditions within the design basis</td><td rowspan="3">Preventive</td><td rowspan="2">Frequent fault</td><td><20mSv on-site
<1mSv off-site
No physical barriers breached where reasonably practicable</td></tr>
<tr><td rowspan="2">3</td><td>DBC-3i</td><td>1E-02 to 1E-03</td></tr>
<tr><td>DBC-3ii</td><td>Infrequent fault</td><td>1E-03 to 1E-04</td><td><200mSv on-site
<10mSv off-site
No more than limited relocation of radioactive material confined by at least one physical barrier</td></tr>
<tr><td rowspan="3">DBC-4</td><td rowspan="3">Protective</td><td>1E-04 to 1E-05</td><td rowspan="3"><500mSv on-site
<100mSv off-site
No more than limited relocation of radioactive material confined by at least one physical barrier</td></tr>
<tr><td rowspan="2">4</td><td>Frequent fault and failure of the first protective measure</td><td rowspan="2"><1E-05</td><td rowspan="2">Note 1</td></tr>
<tr><td>Design Extension Conditions (fault conditions)</td><td>DEC-A</td><td>Control of fault conditions beyond the design basis</td><td>Beyond design basis</td></tr>
<tr><td></td><td>Design Extension Conditions (accident conditions)</td><td>DEC-B</td><td>Control of severe accidents</td><td colspan="2">Mitigating</td><td rowspan="2"></td><td rowspan="2">Note 1</td><td><100mSv off-site
At least one physical barrier intact confining any substantial relocation of radioactive material</td></tr>
<tr><td>5</td><td>N/A</td><td>N/A</td><td>Mitigation of radiological consequences of significant releases of radioactive material</td><td colspan="2">Mitigating</td><td>N/A</td></tr>
<tr><td colspan="9">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.</td></tr>
</table>

3.1.7 Application of General Design Requirements

At PCD, the E3S Design Principles, Reference [3], have been used to guide and inform the ongoing design development process. As part of the systems engineering approach, a comprehensive set of non-functional system requirements (also termed transverse requirements) are being developed from these principles, which will be contained in DOORS and applied to the site, plant, or SSC as part of the requirements definition.

The transverse requirements in development will cover the following E3S design principles (noting this list is non-exhaustive):

1. Simple and forgiving design
    a. Employment of hierarchy of controls
    b. Practical elimination
    c. Fail safe design
2. Design of Safety Class 1 and 2 SSCs for DBCs:
    a. Conservative design to achieve safety functions in most onerous initial conditions and without reliance on other equipment
    b. Tolerance to common cause failures
    c. Redundancy (including tolerance to Single Failure Criterion for Class 1 SSCs, when in the worst permitted configuration of equipment for outages)
    d. Segregation of redundant trains
    e. Diversity of initiation between Safety Measures
    f. Diverse onsite essential services
    g. Deliver 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
    h. Deliver safety functions without reliance on essential services supplied from on-site mobile equipment for 72 hours or from off-site for 7 days
3. Best-estimate design of SSCs for DEC-A and DEC-B:
    a. Design to deliver safety functions following failures consequential upon the initiating event
    b. 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
    c. Design to deliver safety functions following accidental aircraft impact

d. Deliver 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)

e. Deliver 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

f. For DEC-B, tolerance to internal and external hazards

4. General design of SSCs

   a. Application of codes and standards commensurate with safety classification

   b. Qualification to deliver safety functions within environmental conditions, commensurate with safety classification

   c. Design to facilitate Examination, Maintenance, Inspection & Testing (EMIT)

5. Design of site and plant layout:

   a. Segregation of radiation sources from people

   b. Segregation from sources of internal and external hazards

   c. Facilitation and control of access and egress, including in response to initiating events

   d. Facilitation of construction, installation, commissioning, decommissioning, and demolition

Requirements placed on the design will be validated first, and then the design verified against them via the Structured Verification process, the output of which provides substantiation evidence that will be reported in the E3S Case (further details on requirements management are described in E3S Case Chapter 1: Introduction, Reference [1]).

3.1.8 Codes and Standards

The RR SMR Engineering Management Plan, Reference [7], 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.

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:

1. 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

2. The selected codes and standards shall be nuclear-specific, where available and appropriate

3. Each code or standard adopted shall be evaluated to determine its applicability, adequacy, and sufficiency

4. 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)

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

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

7. 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

8. 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)

9. 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

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

11. 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

12. 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

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, Reference [8]. 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, Reference [9]. Further guidance on the implementation of the process for final concept definition will be developed.

A summary of the codes and standards for each discipline at PCD is presented in Reference [8], with applicable codes reported in Section 1 of individual chapters across the E3S Case. The development of RGP for codes and standards is ongoing, and additional design codes and

standards (such as specific codes for mechanical components) will be presented in future revisions of the E3S Case as evidence in the CAE Route Map is developed.

3.1.9 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 described in E3S Case Chapter 15: Safety Analysis, Reference [10].

Deterministic Safety Analysis

Hazards for the RR SMR are identified using a variety of well-established techniques, such as Hazard & Operability (HAZOP) studies, Failure Mode, Effects & 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 (or the Probabilistic Safety Analysis (PSA) model for probabilistic analysis). The sentencing process is based on the severity of their unmitigated consequences or 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 safety case and provides an entry point for exploration of the PIEs and the associated safety functions. 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 computational codes 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 defines the success criteria that must be met at each level of defence-in-depth 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 infrequent faults and

DEC-A/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, including severe accidents (DEC-B) 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 shutdown state.

The initial conditions and key parameters used in the performance analysis will also support definition and substantiation of Operational Limits & Conditions (OLCs), and performance analysis for DECs will support definition of accident management strategies and emergency procedures. Further information on RR SMR deterministic safety methodologies is provided in Reference [4].

Probabilistic Safety Analysis

PSA studies combine IEF information with Safety Measure failure probability information, to evaluate the design against numerical targets listed in Table 3.1-1.

PSA is constructed and iterated throughout the design process, to:

1. Study the benefits and detriments of various design options in support of risk minimisation

2. Evaluate risks to demonstrate they are below numerical targets and are ALARP

3. 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

Internal Hazards

In addition to plant faults, the RR SMR evaluates internal hazards in the context of nuclear safety, 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.

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 covers:

1. Segregation: the internal hazards safety case is largely being built on the concept of segregation of SSCs within the design through physical distance (separation) or physical barriers, undertaking deterministic assessment of hazards to ensure that individual losses of equipment can be tolerated within the Safety Case due to redundant equipment remaining available

2. Identification of Safety Measures: the deterministic assessment process identifies suitable and sufficient safety measures that are aligned with RGP, noting early engagement in the design process seeks to minimise reliance on Safety Measures through design optimisation

The level of assessment undertaken is guided by the frequency of the hazard, similar to plant faults for design basis and beyond design basis regions, noting low frequency high

consequence internal hazards such as turbine disintegration will still receive significant effort to demonstrate a robust safety case. The assessment approach comprises:

1. Identification of hazards
2. Characterisation of hazards in terms of effects on safety plant
3. Consideration of loss of SSCs in relation to the Fault Schedule
4. Identification of hazard protection measures required to ensure sufficient and suitable safety measures remain available
5. Classification of hazard protection measures and definition of safety categorised functional requirements

The assessment process will also consider:

1. Plant operating modes and the availability of systems
2. Single random failures (tolerance to the Single Failure Criterion)
3. 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, and independent hazards whereby there is no causal relationships between the combinations

The outputs are summarised in the Fault Schedule, to provide a key interface between the internal hazard assessment and the requirements placed on the design.

External Hazards

In addition to plant faults, the RR SMR evaluates 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.

For hazards that can be characterised with non-discrete frequency of exceedance hazard curves, the design basis is set based on:

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

Further details on the external hazards and associated parameters defined to support the design of the RR SMR are provided in E3S Case Chapter 2: Generic Site Envelope, Reference [11].

3.2 Categorisation & Classification

3.2.1 Safety Categorisation & Classification

The RR SMR safety categorisation and classification method, justified in Reference [12], is summarised below. It has been developed based on RGP to assign categorisations and classifications, including IAEA guidance, EUR, British Standards (BS EN 61226) and approaches adopted by other vendors within the UK regulatory environment.

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:

1. Category A – any function that plays a principal role in ensuring nuclear safety

2. Category B – any function that makes a significant contribution to nuclear safety

3. 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:

1. Class 1 – any SSC that forms a principal means of fulfilling a Category A function

2. Class 2 – any SSC that makes a significant contribution to fulfilling a Category A function or forms a principal means of ensuring a Category B function

3. 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 3.1.8.

The functions performed by 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 measures in the design is assigned to Category C.

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

Measure and its role in delivering defence in depth		Unmitigated 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* / 1-20mSv *on-site*	0.01 - 0.1mSv *off-site* / 0.1-1mSv *on-site*
Duty	Number measures available to deliver Cat A or Cat B functionality in subsequent levels of DiD	0	A	A	A	B	C
		1	B	B	B	C	C
		2	C	-	-	-	-
Preventive	Number of preventive measures needed to reduce the demand for protective measures in subsequent levels of DiD	0	C	C	C	C	C
		1 when reducing demand to outside of a region requiring protective measures	A	A	A	B	C
		1 when reducing demand from two measures to a single measure	B	-	-	-	-
		2	A+B	-	-	-	-
Protective	Postulated protective measure demand frequency (per year)	>1E-01	A+B	A	A	B	C
		1E-01 – 1E-02	A+B	A	A	B	C
		1E-02 – 1E-03	A+B	A	A	B	-
		1E-03 – 1E-04	A	A	C	-	-
		1E-04 – 1E-05	A	C	C	-	-
		1E-05 – 1E-06	C	C	-	-	-
		1E-06 – 1E-07	C	-	-	-	-
		1E-07 – 1E-08	C	-	-	-	-
		<1E-08	-	-	-	-	-
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 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, Category A functions are delivered by Class 1 SSC, Category B functions are delivered by Class 2 SSC and Category C functions are delivered by Class 3 SSC, as summarised in Table 3.2-2.

Table 3.2-2: 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 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 Class 1, defined as follows:

1. Very High Reliability (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

2. 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 outputs of the application of the categorisation and classification method for each SSC is presented throughout the engineering chapters of the E3S Case. The categorisation and classification method will be developed to incorporate the wider E3S (see Section 3.2.3) and any additional RGP and learning.

3.2.2 Environment, Security, and Safeguards Categorisation & Classification

Methodologies for the categorisation of environment, security and safeguards functions are in development and will be presented in a future revision of the E3S Case as evidence in the CAE Route Map is developed.

3.2.3 Seismic Classification

The RR SMR seismic performance classification method, justified in Reference [13], is summarised below. It 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.

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:

1. 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)

2. 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

3. 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 definitions for DBE and OBE are developed in E3S Case Chapter 2: Generic Site Characteristics, Reference [11]. The seismic performance classification method is summarised in Table 3.2-3.

Table 3.2-3: Relationship between SSC E3S classification and seismic performance classification

SSC E3S Classification	SSC Seismic Performance Classification
1	SPC1
2	SPC1

SSC E3S Classification	**SSC Seismic Performance Classification**
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.

3.3 Conclusions

3.3.1 Conclusions

Evidence is presented to support the overall chapter Claim that 'E3S design principles and associated methods, approaches, and requirements are established for the RR SMR to achieve the E3S fundamental objective', which contributes to the overall E3S objective to protect people and the environment from harm, and the demonstration that risks are reduced ALARP.

E3S Design Principles presented in this report 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.

The principles outlined are based on UK and international RGP, such that they provide a suitable framework for the design and analysis of the RR SMR to achieve its E3S objective 'to protect people and the environment from harm'.

The complete suite of evidence to underpin the Claim will be developed in line with the CAE Route Map and reported in future revisions of the E3S Case, including approaches to derive and categorise environmental, security and safeguards functions, formalisation of non-functional system requirements to be placed onto the design based on the E3S design principles, and further development of codes and standards for application to the design.

3.3.2 Assumptions & Commitments on Future Duty holder

None identified in this revision.

3.4 References

[1] RR SMR Report, SMR0004294/001, “E3S Case Chapter 1: Introduction,” March 2023.
[2] RR SMR Report, SMR0002155/001, “E3S Case CAE Route Map,” March 2023.
[3] RR SMR Report, SMR0001603/001, “Environment, Safety, Security and Safeguards Design Principles,” August 2022.
[4] RR SMR Report, SMR0000531/001, “Deterministic Safety Case - Methodologies,” October 2022.
[5] RR SMR Report, SMR0004520/001, “E3S Case Chapter 18: Human Factors Engineering,” March 2023.
[6] RR SMR Report, SMR0004487/001, “E3S Case Chapter 24: ALARP Summary,” March 2023.
[7] RR SMR Report, SMR0000520/003, “Engineering Management Plan for Rolls-Royce SMR,” October 2022.
[8] RR SMR Report, SMR0003023/001, “Rolls-Royce Small Modular Reactor Codes and Standards,” October 2022.
[9] RR SMR, C3.2.1-2, “DR Process Guidance,” 2022.
[10] RR SMR Report, SMR0003977/001, “E3S Case Chapter 15: Safety Analysis,” March 2023.
[11] RR SMR Report, SMR0004542/001, “E3S Case Chapter 2: Generic Site Characteristics,” March 2023.
[12] RR SMR Report, EDNS01000887611/002, “RR SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method,” August 2021.
[13] RR SMR Report, SMR0001391/001, “Rolls-Royce Small Modular Reactor Seismic Performance Classification Method,” October 2022.

3.5 Appendix A: CAE Route Map

3.5.1 Chapter 3 Route Map

A preliminary Claims decomposition from the overall Chapter 3 Claim is summarised in Table 3.5-1, including the Tier 2 Evidence underpinning the Claims at PCD (i.e., summarised in Revision 1 of this report) and further Tier 2 Evidence still to be developed.

Table 3.5-1: CAE Route Map

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 3**	**Underpinning Tier 2 Evidence** ***at PCD***	**Underpinning Tier 2 Evidence** ***to be developed***
E3S design principles are derived based on UK and international RGP	-	-	-	Section 3.1.1	E3S Design Principles [3]	-
The E3S methods, approaches, and requirements to achieve the E3S	-	-	E3S functions are developed in a structured manner to develop E3S functional requirements for the design	Section 3.1.2	Deterministic Safety Case - Methodologies [4]	Methodologies for environment, security, and safeguards functions (TBC)

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 3	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
fundamental objective are suitably defined	-	-	Numerical dose and risk targets for workers and the public provide the basis for E3S evaluation	Section 3.1.3	E3S Design Principles [3]	-
	-	-	The concept of Defence in Depth to prevent, protect and mitigate failures is adopted in the design	Section 3.1.6	E3S Design Principles [3]	-
	-	-	A set of design requirements are derived for application to the site, plant and SSCs based on the E3S Design Principles, which feed into the requirements verification process	Section 3.1.7	n/a	DOORS Transverse Requirements Module

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 3	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
			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	Section 3.1.8	Engineering Management Plan (codes and standards policy) [7] RR SMR Codes and Standards [8]	Process for Component Standardisation Components and Structures Design Codes & Standards Functional Design Requirements
			Deterministic, probabilistic, internal, and external hazards analysis techniques inform and evaluate the design to demonstrate risks are reduced to ALARP	Section 3.1.9	Deterministic Safety Case - Methodologies [4]	Revised Deterministic Safety Case – Methodologies Methodologies for PSA, Severe Accident Analysis, Internal Hazards Analysis, and External Hazards Analysis

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 3	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *to be developed
			E3S functions are appropriately categorised, with SSCs delivering functions appropriately classified, to inform design requirements	Section 3.2	Environment, Safety, Security and Safeguards Categorisation and Classification Method [12] Seismic Performance Classification Method [13]	Revision 2 of [12] to incorporate all E3S aspects

3.6 Acronyms and Abbreviations

ALARP	As Low As Reasonably Practicable
BS	British Standard
BSL	Basic Safety Level
BSO	Basic Safety Objective
CAE	Claims, Arguments, Evidence
C&I	Control and Instrumentation
CAE	Claim, Argument and Evidence
CDF	Core Damage Frequency
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRM	Confinement of Radioactive Material
DBC	Design Basis Condition
DBE	Design Basis Earthquake
DEC	Design Extension Condition
DiD	Defence in Depth
DNBR	Departure from Nuclear Boiling Ratio
DOORS	Dynamic Object Orientated Requirements System
E3S	Environment, Safety, Security and Safeguards
EA	Environment Agency
EMIT	Examination, Maintenance, Inspection and Testing
EPF	Environmental Protection Function
EPM	Environmental Protection Measure
EUR	European Utility Requirements
FMECA	Failure Mode, Effects & Criticality Analysis
GER	Generic Environmental Report
GSR	Generic Security Report

HAZOP	Hazard & Operability
HF	Human Factors
HLSF	High Level Safety Function
HR	High Reliability
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IEF	Initiating Event Frequency
LRF	Large Release Frequency
OBE	Operating Basis Earthquake
OLC	Operating Limit and Condition
ONR	Office for Nuclear Regulation
PCD	Preliminary Concept Definition
PCSR	Pre-Construction Safety Report
PIE	Postulated Initiating Events
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
RGP	Relevant Good Practice
RR SMR	Rolls-Royce Small Modular Reactor
SAPs	Safety Assessment Principles
SPC	Seismic Performance Class
SSC	System, Structure and Component
Sv	Sievert
SyAPs	Security Assessment Principles
UK	United Kingdom
VHR	Very High Reliability
WENRA	Western European Nuclear Regulators' Association