|  |
| --- |
|  |
| ONR Assessment Report  Generic Design Assessment of the Rolls Royce SMR – Step 2 Assessment of Fault Studies |



ONR Assessment Report

**Project Name**: Generic Design Assessment of the Rolls-Royce SMR

**Report Title**: Step 2 Assessment of Fault Studies

**Authored by**: [Redacted]

**Report Issue No**: 1

**Document ID**: ONRW-2126615823-2793

**Publication Date**: Jun-24

© Office for Nuclear Regulation, 2024

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled. If you wish to reuse this information visit [www.onr.org.uk/copyright](http://www.onr.org.uk/copyright) for details.

# Executive Summary

This report presents the findings of my Fault Studies assessment of the Rolls-Royce Small Modular Reactor (SMR) as part of Step 2 of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA). This assessment is based upon the information presented in version 2 of Rolls-Royce SMR Limited’s Environmental, Safety, Security and Safeguards (E3S) case chapters and supporting documentation.

ONR’s GDA process calls for a step-wise assessment, which increases in detail as the project progresses. The focus of my assessment in this step was towards the fundamental adequacy of the Rolls-Royce SMR design and safety case, and the suitability of the methodologies, approaches, codes, standards and philosophies which form the building blocks for the design and generic E3S case.

I targeted my assessment, in accordance with my assessment plan, at the content of most relevance to Fault Studies against the expectations of ONR’s Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and other guidance which ONR regards as Relevant Good Practice (RGP).

I targeted the following aspects in my assessment of the Rolls-Royce SMR E3S case:

* Adequacy of safety analysis methodologies and principles.
* Adequacy of initiating event and fault sequence identification.
* Adequacy of performance analysis and demonstration of the fault tolerance of the plant.
* Approach to the identification of the safe operating envelope of the plant.

Based upon my assessment, I have concluded the following:

* The RP has developed a suitable set of methodologies that will enable it to deliver adequate design basis analysis in the future. However, I have identified a potential shortfall against UK RGP with regards to assumptions on maintenance restrictions for Class 2 safety measures in the RP’s deterministic analysis and will follow this up in Step 3 as a residual matter.
* The RP has developed a suitable methodology to ensure a graded approach to the categorisation of safety functions and classification of safety measures. The information that has been submitted is largely consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* The RP has presented an appropriate approach to the identification of initiating events in the E3S case which appears systematic, auditable, and comprehensive. However, at this stage in the development of the design and safety case the RP has not identified all potential initiating faults. Whilst additional work is required in Step 3, I consider that the information submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* The RP has presented an appropriate approach to the development of its Fault Schedule. However, at this stage in the development of the design and safety case some elements still require populating. Whilst additional work is required in Step 3, I consider that the information that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* The identification of safety functional requirements, and their decomposition, is an area that requires further development in the RP’s safety case. Insufficient detail has been presented to form a judgement on the approach in Step 2, and I will seek further information with regard to this residual matter in Step 3.
* Whilst additional work is required by the RP in Step 3, I consider that the performance analysis that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* Whilst additional work is required by the RP in Step 3 (and beyond) to validate its codes and methods, I consider that the information submitted to date is consistent with UK RGP and I do not have significant concerns that the RP will be able to further develop the necessary evidence in the future.
* Insufficient detail has been presented in Step 2 to form a judgement on the adequacy of the RP’s radiological consequence analysis for design basis faults and I will seek further information with regard to this residual matter in Step 3.
* The RP has presented suitable consideration of the implications of boron free operation, from a Fault Studies perspective. Although further core design optimisation and analysis work is necessary, I have confidence that acceptable margin may be demonstrated in relevant faults in the future, and I am content with the RP's position for Step 2.
* The identification of operating limits and conditions, and hence the safe operating envelope, is an area that requires further development in the RP’s safety case. Insufficient detail has been presented to form a judgement on the approach in Step 2, and I will seek further information with regard to this residual matter in Step 3.
* With regards to the operational philosophy and overall balance of the generic Rolls-Royce SMR design I have identified potential shortfalls against UK RGP. These shortfalls relate to the classification of the SSCs that support the PDHR safety measure and the commonality of specific SSCs between safety measures. I will therefore follow these residual matters up in Step 3.

Overall, based on my assessment to date, and subject to the provision and assessment of suitable and sufficient supporting evidence, I have not identified any fundamental safety shortfalls that could prevent ONR permissioning the construction of a power station based on the generic Rolls-Royce SMR design.

# List of Abbreviations

ADS Automatic Depressurisation System

ALARP As low as is reasonably practicable

ASD Atmospheric Steam Dump

ASF Alternative Shutdown Function

ATWS Anticipated Transient Without Scram

BSL Basic Safety level (in SAPs)

BSO Basic Safety Objective (in SAPs)

C&I Control and Instrumentation

CoFT Control of Fuel Temperature

CoR Control of Reactivity

DBA Design Basis Analysis

DBC Design Basis Conditions

DEC Design Extension Conditions

DiD Defence-in-Depth

DNB Departure from Nucleate Boiling

DNBR Departure from Nucleate Boiling Ratio

DRP Design Reference Point

DSA Deterministic Safety Assessment

EBD Emergency Blowdown

ECC Emergency Core Cooling

E3S Environment, Safety, Security and Safeguards

GDA Generic Design Assessment

HPIS High Pressure Injection System

IAEA International Atomic Energy Agency

IET Integrated Effects Test

LOCA Loss of Coolant Accident

LOOP Loss of Off-site Power

LPIS Low Pressure Injection System

LUHS Local Ultimate Heat Sink

MSLB Main Steam Line Break

NRW Natural Resources Wales

ONR Office for Nuclear Regulation

PCC Passive Containment Cooling

PDHR Passive Decay Heat Removal

PIE Postulated Initiating Event

PSA Probabilistic Safety Assessment

PSCS Passive Steam Condensing System

PWR Pressurised Water Reactor

RCP Reactor Coolant Pump

REA Rod Ejection Accident

RAPFE Radial Averaged Peak Fuel Enthalpy

RGP Relevant Good Practice

RP Requesting Party

RPV Reactor Pressure Vessel

SAA Severe Accident Analysis

SAP Safety Assessment Principle(s)

SBO Station Blackout

SET Separate Effects Test

SFAIRP So far as is reasonably practicable

SG Steam Generator

SGTR Steam Generator Tube Rupture

SMR Small Modular Reactor

SSC Structure, System and Component

TAG Technical Assessment Guide(s) (ONR)

TSC Technical Support Contractor

V&V Verification and Validation

WENRA Western European Nuclear Regulators’ Association

Contents

[Executive Summary 3](#_Toc169530830)

[List of Abbreviations 6](#_Toc169530831)

[1. Introduction 9](#_Toc169530832)

[2. Assessment standards and interfaces 12](#_Toc169530833)

[3. Requesting party’s submission 16](#_Toc169530834)

[4. ONR assessment 23](#_Toc169530835)

[5. Conclusions 43](#_Toc169530836)

[References 46](#_Toc169530837)

[Appendix 1 – Relevant SAPs considered during the assessment 52](#_Toc169530838)

# Introduction

1. This report presents the outcomes of my Fault Studies assessment of the generic Rolls-Royce Small Modular Reactor (SMR) design, as part of Step 2 of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA). This assessment is based upon the information presented in version 2 of Rolls-Royce SMR Limited’s Environmental, Safety, Security and Safeguards (E3S) case chapters (refs [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], and [11]), and supporting documentation.
2. Assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) Management System and follows ONR’s guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [12]). The ONR Safety Assessment Principles (SAPs) (ref. [13]), together with supporting Technical Assessment Guides (TAGs) (ref. [14]), have been used as the basis for this assessment.
3. This is a Major report, as defined in NS-TAST-GD-108 (ref. [15]).

## Background

1. The ONR’s GDA process (ref. [16]) calls for a step-wise assessment of the Requesting Party's (RP) submissions with the assessments increasing in detail as the project progresses. Rolls-Royce SMR Limited is the RP for the GDA of the Rolls-Royce SMR design.
2. In April 2022 ONR, together with the Environment Agency and Natural Resources Wales (NRW), began Step 1 of the GDA for the generic Rolls-Royce SMR design. Step 1, which is the preparatory part of the design assessment process and mainly associated with initiation of the project and preparation for technical assessment in later steps, was successfully completed in 12 months.
3. Step 2 commenced in April 2023. This is the first substantive technical assessment step. The focus of ONR’s assessments in this step is towards the fundamental adequacy of the design and safety and security cases, and the suitability of the methodologies, approaches, codes, standards and philosophies which form the building blocks for the design and generic safety and security cases. The objective is to undertake an assessment of the design against regulatory expectations to identify any fundamental safety or security shortfalls that could prevent ONR permissioning the construction of a power station based on the design.
4. Prior to the start of Step 2 I prepared a detailed Assessment Plan for Fault Studies (ref. [17]). This has formed the basis of this assessment and was also shared with the RP to maximise openness and transparency.
5. This report is one of a series of Assessments which support ONR’s overall judgements at the end of Step 2 which are recorded in the Step 2 Summary Report (ref. [18]).

## Scope

1. The assessment documented in this report is based upon the E3S case for the Rolls-Royce SMR as summarised in the E3S case chapters and supporting documentation.
2. The overall scope of the Rolls-Royce SMR GDA is described in (ref. [19]). Rolls-Royce SMR Limited has indicated that it intends to complete a three step GDA, with the objective of receiving a DAC from ONR and have aligned their GDA scope with this objective. The GDA scope defines the generic plant and layout and includes all systems, structures and components that are identified as being important to environment, safety, security and safeguards, all modes of operation, and all stages of the plant lifecycle.
3. However, given the step-wise assessment during GDA, information has not been submitted for all aspects within the GDA Scope during Step 2. The following aspects of the E3S case are therefore out of scope of this assessment:

* Analysis of faults arising during low power and in shutdown. The RP has prioritised a subset of at power reactor faults for preliminary analysis. A full suite of reactor fault analyis will be presented in Step 3. The RP argues it is logical to sequence the analysis with initial focus on full power faults, on the assumption that protection against faults at low power or in shutdown will be straightforward to substantiate due to the lower decay heat. Although I consider this position to be reasonable for Step 2, significant work will be required to demonstrate this.
* Analysis of spent fuel pool and fuel route faults. In Step 2, the RP has perfomed intial fault and hazard identification studies for this category of faults, however a full suite of non-reactor fault analysis will not be presented until Step 3. Although I consider this to be sufficent for Step 2, the RP’s approach to focus on reactor faults is based on the assumption that protection against spent fuel pool and fuel route faults will be less onerous to substantiate due to the relative simplicity of the systems (when compared to the reactor protection systems). Significant work is still required to demonstrate this.
* Validation evidence to support the RP’s choice of Codes and Methods for the analysis of thermal hydraulic and reactor physics. However, whilst experimental data from test rigs will not be produced on the timescales of GDA, I have considered the RP’s strategy for demonstrating the verification and validation (V&V) of plant performance codes and methods.
* Whilst the implications of boron free operation with respect to power excursion in reactivity faults is of significance for Fault Studies, implications for the design of the core are within the scope of the F&C assessment (ref. [20]). Implications relating to waste streams are within the scope of the Environment Agency assessment. The safety justification for the primary circuit chemistry and the impacts of this operating chemistry choice on the generation, transport and behaviour of radioactivity are within scope of the chemistry assessment (ref. [21]).

1. My assessment strategy, which is detailed in sub-section 4.1, has considered the following fundamental aspects of the RP’s safety case:

* Adequacy of safety analysis methodologies and principles. The RP claims that an appropriate set of principles are applied to the design and analysis of Structures, Systems and Components (SSCs); and that conservative analysis methods are used to inform and evaluate the design, and demonstrate suitable margins to avoid cliff-edge effects.
* Adequacy of initiating event and fault sequence identification. The RP claims that all credible Postulated Initiating Events (PIEs) associated with operation of the generic Rolls-Royce SMR design are identified, fully defined and sentenced appropriately for analysis.
* Adequacy of the performance analysis and demonstration of the fault tolerance of the plant. The RP claims that the computer codes and models employed for performance analysis are validated for their chosen application, and that deterministic analysis demonstrates that all identified safety criteria are met.
* Approach to the identification of Operating Rules, and hence the safe operating envelope of the plant. The RP claims that the operating assumptions, limits and conditions set by fault analysis are appropriately captured.

# Assessment standards and interfaces

1. For ONR, the primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a safety, security and safeguards case for the reactor technology being assessed.
2. ONR has a range of internal guidance to enable Inspectors to undertake a proportionate and consistent assessment of such cases. This section identifies the standards which have been considered in this assessment.
3. This section also identifies the key interfaces with other technical topic areas.

## Standards

1. The ONR Safety Assessment Principles (SAPs) (ref. [13]) constitute the regulatory principles against which the RP’s case is judged. Consequently, the SAPs are the basis for ONR’s assessment and have therefore been used for the Step 2 assessment of the Rolls-Royce SMR.
2. The International Atomic Energy Agency (IAEA) safety standards (ref. [22]) and nuclear security series (ref. [23]) are a cornerstone of the global nuclear safety and security regime. They provide a framework of fundamental principles, requirements and guidance. They are applicable, as relevant, throughout the entire lifetime of facilities and activities.
3. Furthermore, ONR is a member of the Western European Nuclear Regulators Association (WENRA). WENRA has developed Reference Levels (ref. [24]), which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors (ref. [25]).
4. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the TAGs (ref. [14]). The TAGs provide the principal means for assessing the Fault Studies aspects in practice.

### Safety Assessment Principles (SAPs)

1. My judgements have been made against the 2014 Edition, Revision 1 (January 2020) version of ONR’s SAPs (ref. [13]).
2. In particular I have made judgements against the fault analysis SAPs (FA series) as these relate to the identification of initiating faults, performance of Design Basis Analysis (DBA), demonstration that appropriate safety measures have been identified, and that the identified measures are effective in mitigating fault consequences. I have also considered the RP’s assurance and validity of data and models as per the intent of the AV series of SAPs.
3. In addition, I have considered the engineering principles SAPs (EKP, ECS and EDR series). These relate to the fault tolerance of the design, defence-in-depth (DiD), the categorisation and classification of safety functions and safety measures, and design for reliability.
4. A list of the SAPs used in this assessment is recorded in Appendix 1.

### Technical Assessment Guides (TAGs)

1. The following TAGs have been used as part of this assessment:

* NS-TAST-GD-005 - Regulating duties to reduce risks to ALARP (ref. [26])
* NS-TAST-GD-006 - Design Basis Analysis (ref. [27])
* NS-TAST-GD-035 - The limits and conditions for nuclear safety (operating rules) (ref. [28])
* NS-TAST-GD-042 - Validation of Computer Codes and Calculation Methods (ref. [29])
* NS-TAST-GD-051 - The purpose, scope and content of safety cases (ref. [30])
* NS-TAST-GD-094 - Categorisation of Safety Functions and Classification of Structures, Systems and Components (ref. [31])
* NS-TAST-GD-096 - Guidance on the Mechanics of Assessment (ref. [12]).

### National and international standards and guidance

1. The following international standards and guidance have been used as part of this assessment:

* IAEA, Fundamental Safety Principles, Safety Fundamentals No. SF-1 (ref. [32]).
* IAEA, Safety Assessment for Facilities and Activities, General Safety Requirements (GSR) Part 4 (ref. [33]).
* IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (ref. [34]).
* IAEA, Deterministic safety analysis for nuclear power plants, Specific Safety Guide No. SSG-2 (ref. [35]).
* IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide No. SSG-30 (ref. [36]).
* IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61 (ref. [37]).
* IAEA, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Specific Safety Guide No. SSG-70 (ref. [38]).

## Integration with other assessment topics

1. I have worked closely with other topics (including Environment Agency and NRW assessors) as part of my Fault Studies assessment. Similarly, other assessors sought input from my assessment. These interactions are key to the success of GDA to prevent or mitigate any gaps, duplications or inconsistencies in ONR’s assessment.
2. The key interactions with other topic areas were:

* Probabilistic Safety Analysis (PSA), with regards to the adequacy of the RP’s approach to:
  + Fault and hazard identification;
  + Determination of initiating event frequency; and
  + Bounding, grouping, and screening of fault sequences for further analysis.
* Fuel & Core, with regards to the adequacy of the RP’s approach to:
  + Identification of fuel performance acceptance criteria;
  + Reactor core design (geometry, loading pattern, control rod positioning, fuel cycles etc.,); and
  + Derivation of fuel performance correlations.
* I have also worked closely with Severe Accident Analysis (SAA), Radiological Consequences (RadCons) and Internal Hazards to ensure consistency in safety analysis assumptions and adequate consideration of implications from these topics on Fault Studies.
* Interaction has been required with most other technical areas to gain confidence in the RP’s approach to categorisation and classification of safety functions and SSCs, and that safety measures can deliver the safety function required of them, as assumed in the fault analysis (e.g., Electrical Engineering, Control and Instrumentation (C&I), Human Factors, Mechanical Engineering, Civil Engineering, Structural Integrity).

## Use of technical support contractors

1. During Step 2 I engaged Technical Support Contractors (TSCs) to support the following specific aspects of my assessment of Fault Studies for the Rolls-Royce SMR:

* A review of the RP’s strategy for the validation of computer codes and methods. This work package covers the computer codes used for Design Basis Analysis (DBA), Fuel and Core, PSA and SAA.

1. The TSCs provided me with technical advice and supported my assessment, working under my close direction and supervision. It should be noted that all regulatory judgements have been made exclusively by ONR.

# Requesting party’s submission

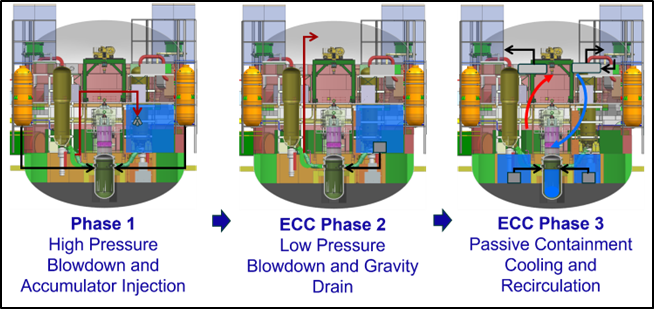
1. Rolls-Royce SMR Limited submitted a series of E3S chapters, or summary reports, and other supporting references, which outline the E3S case for the generic Rolls-Royce SMR design. This section presents a summary of the RP’s safety case for Fault Studies. It also identifies the documents submitted by the RP which have formed the basis of my Fault Studies assessment of the Rolls-Royce SMR design.

## Summary of the Rolls-Royce SMR design

1. The generic Rolls-Royce SMR design is a three loop Pressurised Water Reactor (PWR) with a target electrical power output of 470 MWe (from a thermal power of 1,358 MWth) and a design life of 60 years for non-replaceable components.
2. The Rolls-Royce SMR design has been developed by the RP based upon well-established PWR technology, in use all over the world. Innovation comes in the form of its modular approach to construction which would see the majority of the power station built in factory conditions and assembled on site.
3. The reactor itself is of a typical PWR design, including a steel Reactor Pressure Vessel (RPV) holding fuel assemblies, Steam Generators (SG), Reactor Coolant Pumps (RCP) and piping, all held within a steel containment vessel. The reactor is equipped with a number of supporting systems for normal operations and a range of safety measures are present in the design to provide cooling, control criticality and contain radioactivity under fault conditions. Passive safety features are preferred to active components, reflecting the RP’s design philosophy.
4. The generic Rolls-Royce SMR design provides four key protective safety measures[[1]](#footnote-2) for the ‘control of reactivity’ (CoR) and ‘control of fuel temperature (CoFT)’ fundamental safety functions. These are:

* Emergency Core Cooling (ECC);
* Passive Decay Heat Removal (PDHR);
* Scram [[2]](#footnote-3); and
* The Alternative Safety Function (ASF).

1. Each safety measure comprises multiple SSCs, and the E3S case refers to different variants of these safety measures which depend upon the plant state at the time they are called upon, the accident, and plant configuration. A high-level summary of each of these four key safety measures follows.
2. The ECC provides the ‘first’[[3]](#footnote-4) protective safety function for loss of coolant accidents and the ‘second’[[4]](#footnote-5) protective safety function for all frequent faults (including intact circuit faults). It provides the principal means of delivering the heat removal safety function and so is a Class 1 safety measure, with three trains (described by the RP as providing N + 2 redundancy). ECC is claimed as a passive system in that following initiation (at which time signals are required to operate valves) no power nor operator action is required for a period of at least 24 hours.
3. The safety measure acts in three phases, depicted in Figure 1. Phase 1 entails depressurisation of the primary circuit via the Automatic Depressurisation System (ADS) and accumulator injection. Phase 2 consists of water inventory from the refuelling pool draining via gravity to the reactor. Phase 3 relies on passive recirculation of condensate within containment via the Passive Containment Cooling (PCC) heat exchangers, cooled by Local Ultimate Heat Sink (LUHS) tanks.



**Figure 1 – Phased ECC Operation** (ref. [39])

1. The PDHR provides the first protective safety function for all frequent faults (and for infrequent intact circuit faults), providing a significant role in delivering the heat removal safety function. Whilst it is the first to act in all frequent faults, since ECC provides the principal means of heat removal for all faults, PDHR is a Class 2 safety measure. ECC is designed to initiate upon failure of PDHR.
2. Despite the name, PDHR comprises active systems in most of its documented variants. The key SSC claimed as part of this safety measure are:
3. High Pressure Injection System (HPIS), which is a two-train (N + 1) pumped system required to maintain primary circuit inventory during Small Un-isolable Loss of Coolant Accidents (LOCA) and mitigate primary circuit contraction as a result of cooldown.
4. The Passive Steam Condensing System (PSCS) which, following actuation establishes natural circulation from the secondary side of the SGs via heat exchangers in the LUHS tanks to remove decay heat. The PSCS is a three-train system (N + 2 redundancy).
5. Scram provides the first protective safety function for delivering control of reactivity and is a Class 1 safety measure. Scram is essentially a passive safety measure, following the signals required for actuation. Due to the absence of soluble boron in the primary circuit during normal operations, the generic Rolls-Royce SMR has been designed to provide full shutdown margin using control rods alone. A design choice that has led to a greater number of control rods being present than in other similar civil PWRs.
6. The ASF provides the second protective safety function for delivering control of reactivity. This safety function is delivered by a Class 2 active safety measure, comprising the HPIS and the Emergency Boron Injection (EBI) system which controls reactivity via the injection of boron-10 enriched potassium tetraborate solution into the core.

## E3S case approach and structure

1. Rolls-Royce SMR Limited has chosen to develop its cases in a holistic manner, as an Environment, Safety, Security and Safeguards (E3S) case. The overall objective for the E3S case is to demonstrate that the design will ‘protect people and the environment from harm’.
2. This means that, although the case made for each of the E3S purposes (i.e., environment, safety, security and safeguards) will inevitably be different at the top level, it will draw upon common evidence outputs (as well as other non-common outputs) to substantiate each of the purposes. This is claimed to offer benefits in terms of clarity, integration and understanding impacts from any changes to the case.
3. The E3S case is being developed using a three-tier hierarchy and incorporating a Claim, Argument and Evidence (CAE) structure with the highest-level claims being derived from the RP’s own E3S principles. The highest level of the three tiers is the RP’s Tier 1 E3S chapters, with the lower tiers providing more detailed arguments and evidence. This is illustrated in Figure 2.

****

**Figure 2: Claim, Argument and Evidence (CAE) structure within the E3S hierarchy** (ref. [1])

1. The structure of the E3S case largely aligns with the IAEA guidance for safety cases, SSG-61 (ref. [37]), supplemented to include UK specific expectations and expanded to include the other E3S purposes.

## Summary of the requesting party’s E3S case for Fault Studies

1. The aspects covered by the Rolls-Royce SMR safety case in the area of Fault Studies can be broadly grouped under four headings, which are summarised as follows:

### Safety analysis methodologies and principles

1. The RP claims that an appropriate set of principles are applied to the design and analysis of SSCs; and that conservative analysis methods are used to inform and evaluate the design and demonstrate suitable margins to avoid cliff-edge effects.
2. The arguments and evidence to support this are presented in a suite of Tier 2 submissions covering design principles, the approach to categorisation and classification, and methodologies for design basis analysis. These together explain the RP’s approach to delivering a comprehensive and robust set of safety analysis to underpin its claims in Chapter 15 of the E3S case (ref. [8]).

### Initiating event and fault sequence identification

1. The RP claims that all credible Postulated Initiating Events (PIEs) associated with operation of the generic Rolls-Royce SMR design are identified, fully defined and sentenced appropriately for analysis.
2. The arguments and evidence to support this are presented in a suite of Tier 2 and 3 submissions, which are argued to demonstrate that a systematic process has been employed to review the developing design and ensure a comprehensive list of Postulated Initiating Events (PIE) for further analysis.

### Performance analysis

1. The RP claims that the computer codes and models employed for performance analysis are validated for their chosen application, and that deterministic analysis demonstrates that all identified safety criteria are met.
2. The arguments and evidence to support this are presented in a suite of Tier 2 and 3 validation and transient analysis reports.

### Safe operating envelope

1. The RP claims that the operating assumptions, limits and conditions set by the RP’s fault analysis are appropriately captured.

## Basis of assessment: requesting party’s documentation

1. The principal documents that have formed the basis of my Fault Studies assessment of the E3S case are:

* Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards (E3S) case, Chapter 15 (ref. [8]).
* Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards (E3S) case, Engineered Safety Features, Chapter 6 (ref. [6]).
* Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles (ref. [40]) – this document provides a set of E3S principles that are used to guide the design of the Rolls-Royce SMR.
* Rolls-Royce SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method (ref. [41]) – this report presents the RP’s methodology for categorisation and classification of safety functions and SSCs.
* Rolls-Royce SMR Deterministic Safety Case – Methodologies (ref. [42]) – this report presents the RP’s methodologies for undertaking design basis Deterministic Safety Assessment (DSA).
* Rolls-Royce SMR Hazard Log Report – Version 7 (ref. [43]) – this report describes the RP’s development of the hazard log, which summarises all hazards identified for the Rolls-Royce SMR, from all inputs (e.g. HAZOPs, FMEA, internal/external hazards etc.)
* Rolls-Royce SMR Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies (ref. [44]) – this report groups hazards identified in the Hazard Log and identifies PIEs that are used for both the design basis and PSA. Initiating event frequencies are also assigned in this report.
* Rolls-Royce SMR Fault Schedule (Version 7) (ref. [45]) – this report describes the Rolls-Royce SMR fault schedule which summarises the identified fault groups and the preventative, protective and mitigative safety measures provided for each.
* Reactor Plant Performance Design Basis Analysis Methodology (ref. [46]) – this report summarises the important safety criteria, analysis assumptions and the calculation route for each fault.
* Reactor Plant Performance Fault Study Analysis Summary (ref. [47]) – this report presents the deterministic analysis for the design basis reactor faults performed to date.
* Design Basis Deterministic Safety Assessment Summary (ref. [48]) – this report summarises the deterministic safety case aspects for each fault (e.g., application of design basis rules, diversity for frequent faults etc.).
* Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Strategy (ref. [49]) – this report summarises the RP’s approach to verification and validation for all of the thermal hydraulics codes used to support its safety case.
* Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Summary (ref. [50]) – this report summarises the verification and validation status of the codes used to support design basis analysis.
* Various Safety Measure Design Definition (SMDD) reports for the key safety systems. These SMDD reports are consistent with the design described in the DRP1 report (ref. [51]). Of particular significance were those for:
  + Emergency Core Cooling (ECC) (ref. [52]);
  + Passive Decay Heat Removal (PDHR) (ref. [53]);
  + Scram (ref. [54]); and
  + The Alternative Shutdown Function (ASF) (ref. [55]).
* ALARP Summary Report – this report presents a summary of the RP’s arguments as to how the generic Rolls-Royce SMR design reduces risks to ALARP at Reference Design seven (RD7) (Ref. [56]).

# ONR assessment

## Assessment strategy

1. My assessment has followed the GDA Step 2 Assessment Plan for Fault Studies [17]. This strategy has sought to target matters which allow me to form a judgement on the fundamentals of the Rolls-Royce SMR design and help to inform ONR’s decision on whether to proceed to Step 3 of the GDA. As such, I have chosen to proportionately target the following aspects of the RP’s E3S case:

* Deterministic safety analysis methodology and design principles.
* Categorisation of safety functions and classification of SCCs.
* Initiating event and fault sequence identification.
* Fault schedule maturity, and the approach adopted for its development.
* Identification of safety functional requirements.
* Performance analysis. Noting that only a preliminary subset of bounding transients has been submitted during Step 2.
* The RP’s strategy for V&V of the codes and methods that will be used in the performance analysis of relevant safety systems.
* The RP’s approach to RadCons for comparison against ONR SAP Numerical Target 4.
* Implications of boron free operation with respect to power excursion and relevant acceptance criteria in reactivity faults.
* The RP’s approach to the identification of operating rules, and hence the safe operating envelope of the plant.

1. I have taken a sampling approach for my assessment to inform a judgement on the adequacy of the RP’s submissions within my assessment scope, in line with ONR policy [12]. The information presented in the Tier 1 E3S case chapters appears consistent with the Tier 2 and 3 submissions I have sampled for assessment.
2. My assessment has targeted the principal and significant means of delivering control of heat removal and reactivity for all faults. Specifically, I have targeted the ECC, PDHR, reactor Scram and ASF.
3. As described in section 2 of this report, I have considered both UK regulatory and international Relevant Good Practice (RGP) to inform my assessment and judgements.

## Assessment

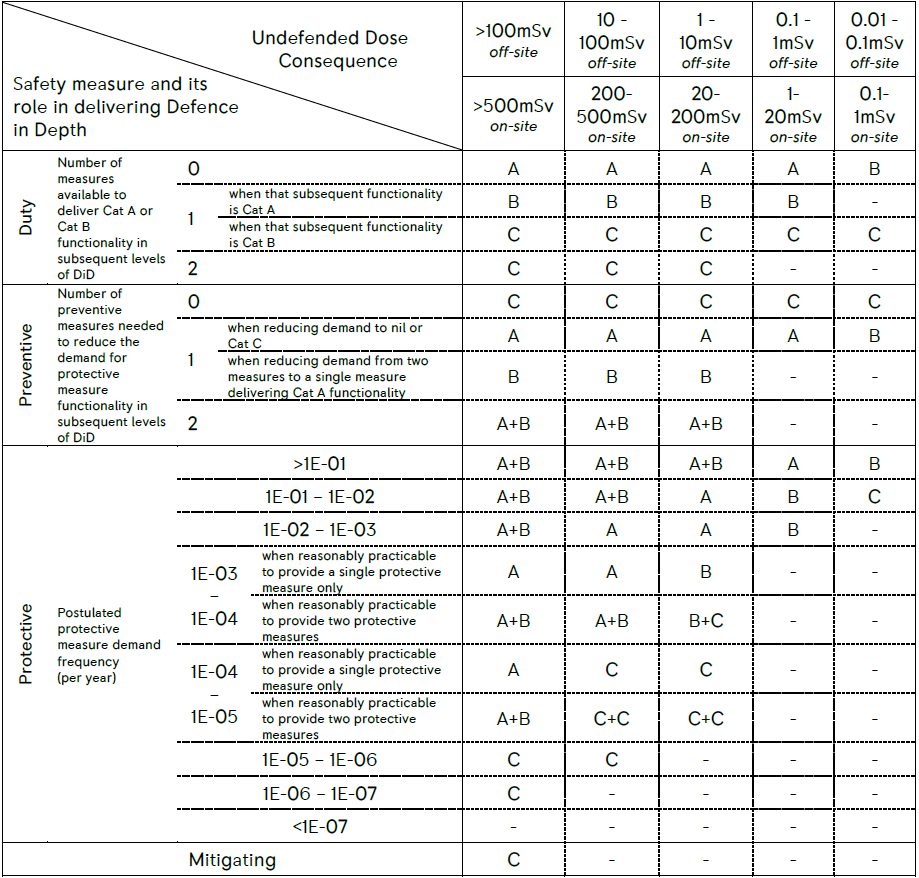
### Safety analysis methodology and principles

1. It is ONR’s expectation that the RP provides justification for its approach to performing deterministic analysis of design basis faults. Such expectations are informed by ONR SAPs FA.4 – FA.9 (ref. [13]), NS-TAST-GD-006 (ref. [27]), IAEA safety requirements SSR-2/1 (ref. [34]) and IAEA safety guide SSG-2 [35]. In this section, I consider the RP’s approach to performing deterministic analysis of design basis faults and defining acceptance criteria.
2. The RP has developed a methodology for performing deterministic analysis. This methodology is presented in a suite of Tier 2 submissions (refs. [42], [46] and [48]), and is augmented by a set of E3S design principles (ref. [40]). These documents together explain the RP’s strategy for delivering a comprehensive and robust set of safety analysis to underpin claims in Chapter 15 of the E3S case (ref. [8]), with regard to the fault tolerance of the design and the effectiveness of safety measures (as per FA.4). However, I consider that further evidence, in the form of transient analysis, will be required to demonstrate that these claims have been substantiated in the future (as discussed in Section 4.2.6).
3. ONR’s SAP FA.5 (ref. [13]) sets expectations related to which faults should be considered for design basis analysis, based on the predicted frequency of occurrence and unmitigated radiological consequences. The initiating event frequency of a design basis fault should be calculated on a best estimate basis and NS-TAST-GD-006 (ref. [27]) also notes that for less frequent initiating events it may be acceptable to relax some acceptance criteria.
4. The RP categorises faults lying in the design basis region in to a series of plant states, or ‘design basis conditions’ (discussed in Section ‎4.2.3). Acceptance criteria are then defined for each category which are proportionate to the decreasing plant state frequency. This is a common approach and is articulated in SSG-2 (ref. [35]). Based on the RP’s definition of plant states in (ref. [40]), I am content that the approach to categorising design basis faults is consistent with the expectations of FA.5 and NS-TAST-GD-006 .
5. The RP differentiates between frequent and infrequent faults with frequent faults being those with a frequency of occurrence greater than 10-3 per annum (pa). The distinction between frequent and infrequent faults is a common approach in the UK to inform deterministic rules for the number of safety systems required in a given scenario. The RP also acknowledges this expectation, and plans (in a departure from the expectations set out in SSG-2) that sequences in which the first line of protection has failed will be considered within the design basis. I am content that this meets the expectation that design basis techniques are applied with a cut-off frequency of around 10-7 pa (SAP FA.6) and consider it an important aspect of demonstrating the fault tolerance of the Rolls-Royce SMR design.
6. It is well established good practice, in design basis analysis, to consider the most limiting random single failure within a safety system (FA.6 and NS-TAST-GD-006). Together with assumptions regarding losses consequential to the initiating event and unavailability due to maintenance, consideration of the single failure criterion determines the required number of independent, redundant trains provided within a safety system. The RP has established a set of safety measure design principles (ref. [40]) which outline the intent to design safety measures to meet these expectations. Additionally, general design basis assumptions employed in the RP’s plant performance analysis regarding (amongst other things) common cause failures, consequential failures, Loss of Off-site Power (LOOP), preventative maintenance and single failure are discussed in (ref. [46]).
7. In my opinion, the RP’s intended design basis rules and assumptions for single failure are aligned with the expectation of SAPs FA.6 and EDR.4. However, I note that whilst the RP’s design principles (ref. [40]) specify that Class 1 safety measures should be designed to accommodate the worst normally permitted configuration for maintenance, this requirement is not made for Class 2 safety measures. Given my expectation that design basis techniques are applied to fault sequences with frequencies down to 10-7 pa, I consider that design basis methodologies, such as assumptions on maintenance test or repair, should apply to analysis of both the principal and diverse means of protection for frequent faults. The RP’s design basis analysis methodology (ref. [46]) states that there will be no maintenance of safety systems that may impact the fault analysis during powered operations, and so the fundamental acceptance of the reactor design would not be undermined. However, the safety case for shutdown states, fuel handling and spent fuel cooling has not been presented in Step 2 and I consider that it is in these aspects of the design that challenges to the necessary redundancy of active safety systems and their essential support services may arise. This represents a potential shortfall against RGP, and I will continue to explore this, and its impacts on the generic Rolls-Royce SMR design, in Step 3.
8. For each category of fault, the RP has assigned a set of acceptance criteria. Each fault is allocated to a plant state, informed by its IEF. At the highest level, these Plant States and acceptance criteria are documented in (ref. [40]), and meet my expectations informed by the Basic Safety Level (BSL) of SAPs Target 4. These high-level criteria are then decomposed into safety limits, or ‘decoupling criteria’, that may be applied in the performance analysis.
9. ONR does not define the safety limits to be used for reactor faults but SAP FA.7 sets the expectation that no barriers (to the release of radioactive material) fail, or if they do a barrier remains without a challenge to its integrity. The overriding expectation is that risks are reduced ALARP. The RP’s safety limits for fuel are reported in the Fuel Design Limits Report (ref. [57]) and the adequacy of these is within the scope of the Fuel and Core assessment (ref. [20]). The RP defines limits for Departure from Nucleate Boiling (DNB) which increase as the plant state category increases. This is a common approach and has been taken in previous GDAs. However, although the RP includes these acceptance criteria, they also acknowledge the expectation that risks are reduced ALARP. Therefore, at this stage, I do not have any specific concern that the RP’s approach to identifying appropriate acceptance criteria will lead to a position where the risk of fuel failures is not reduced ALARP.
10. The RP’s submissions recognise the need to link design basis transient analysis and radiological consequences. My assessment of the RP’s approach to radiological analysis is summarised in Section 4.2.8, and so not discussed further in this section.
11. Overall, I am broadly content that the RP’s deterministic safety analysis methodology and principles will deliver adequate design basis analysis to support the E3S case. However, I have identified a potential shortfall against UK RGP with regards to assumptions on maintenance restrictions for Class 2 safety measures, and I will follow this up as a residual matter in Step 3.

### Categorisation and classification methodology

1. SAPs EKP.4 and ECS.1 set ONR’s expectations that safety functions will be identified and categorised based on their significance to safety. SAPs EKP.5 and ECS.2 set the expectation that SSCs will be identified and classified on the basis of those functions and their significance to safety. These expectations are further developed in ONR’s TAG NS-TAST-GD-094 (ref. [31]) and broadly aligned with the guidance in IAEA Specific Safety Guide, SSG-30 (ref. [36]). I have therefore sought to gain confidence that the RP’s method for the categorisation of safety functions and classification of SSCs is appropriate and consistent with the approach to DBA.
2. During Step 2, the RP has not presented a holistic and systematic decomposition of safety functions (discussed further in Section 4.2.5). My assessment, therefore, has been limited to the application of the categorisation and classification methodology at a high level. I will revisit this in my Step 3 assessment.
3. The RP claims that its methodology for the categorisation of safety functions and the classification of SSCs (ref. [41]), is based upon RGP in multiple sources of guidance such as ONR SAPs and TAGs, IAEA Safety Guides and Techdocs, European Utility Requirements (EURs), British Standards and industry standards (Safety Directors Forum position papers). I consider that the use of these established standards provides a sound foundation to the development of an adequate categorisation and classification process and, at a high level is likely to be consistent with the expectations of EKP4, EKP.5, ECS.1 and ECS.2.
4. The RP’s process described in (ref. [41]) provides a scheme for categorising protective safety functions (Level 3 DiD) across a range of frequency and unmitigated dose bands. The categorisation of duty (Level 1 DID) and preventative (Level 2 DiD) safety functions is then dependent upon what the RP considers achievable with regards to the protective level of DiD. Table 1 summarises the RP’s process for categorisation of the functions performed by safety measures over the various levels of the DiD hierarchy.
5. For all faults, at least one Cat A, B or C safety function will be identified at either the duty, preventative or protective level of DiD. However, the process places the emphasis on protective safety measures and leads to an uprating of preventative and duty safety measures if protective safety measures cannot be identified. Although there are exceptions to this where there is precedent in RGP. For example, the reactor coolant system is identified as delivering a Cat A safety function. However, the categorisation of the protective safety functions for failure of the reactor coolant system are not downgraded and remain at Cat A (+ B for frequent faults).

**Table 1 – The RP’s Scheme for Categorisation of the Functions Performed by Safety Measures** (ref. [41])



1. It can be seen from Table 1 that in the RP’s scheme, a frequent initiating event with a large unmitigated dose consequence requires two safety measures, one delivering a Category A safety function and the other delivering a Category B safety function. This is consistent with the principles set out in NS-TAST-GD-094.
2. It can also be seen from Table 1 that the RP’s scheme employs finer granularity in the frequency ranges than the indicative scheme in NS-TAST-GD-094. Within the region of 1 to 10-3 pa, the methodology indicates a reduced need for a diverse safety function with lower radiological consequences. In my opinion, this is a shortfall against the expectations that two lines of protection are provided for frequent faults, articulated in NS-TAST-GD-006. Although I note that additional safety measures at the preventative and duty levels of DiD would be identified following the scheme in Table 1. Furthermore, I consider that the affected region is most likely to be associated with non-reactor faults and therefore, in my opinion, does not represent a challenge to the fundamental adequacy of the reactor design for Step 2. I will however follow up the implications of this for fuel handling and spent fuel pool faults during my Step 3 assessment.
3. The RP’s scheme also allows for the initial categorisation of a safety function to be downrated over time (as the plant moves into a safer and more controlled state) where a working medium is consumed in delivering safety measure functionality. In such cases the means of replenishing the working medium may be downrated to the next safety function category and so the required classification of the SSCs tasked with delivery of the safety function may be downrated accordingly. I note that SSG-30 (ref. [36]) discusses time related aspects of refinement to categorisation and classification in the context of plant states following an accident[[5]](#footnote-6) and consider this leads to similar outcomes. As such, the RP’s scheme is generally consistent with the approach adopted in previous GDAs in that either lower classification systems or multiple divisions of the class 1 system are credited once the ‘controlled state’ has been reached. Ultimately, the licensee needs to demonstrate that the plant can be brought to a stable, safe state and there is flexibility in how any categorisation and classification methodology may be formulated to help achieve this.
4. For the reactor, the RP’s methodology results in Category A safety functions being assigned to the ECC and Scram, and Category B safety functions being assigned to PDHR and ASF. Whilst the RP’s scheme broadly aligns with my expectations for categorisation and classification, in my opinion, the categorisation of PDHR does not align with my expectations for the prevention of the failure of barriers to release, as its failure in an Intact Circuit Fault (ICF) would lead to initiation of the ECC and depressurisation of the primary circuit. This aspect of the RP’s operational philosophy is discussed further in section 4.2.11.
5. The application of the RP’s methodology will be a focus of my assessment during Step 3, particularly with regard to non-reactor faults, where calculations of unmitigated consequence are likely to be of greater importance in determining the safety functions assigned to various faults.
6. Overall, I am broadly content that the scheme adopted by the RP for the Rolls-Royce SMR safety case provides a graded approach to the categorisation of safety functions and classification of safety measures. The information that has been submitted is largely consistent with UK RGP and should enable the RP to further develop its generic Rolls-Royce SMR design and associated E3S case evidence. I therefore judge, that for Step 2, the RP’s methodology meets my expectations, as informed by ECS.1 and ECS.2, but that appropriate demonstration of its application will be necessary in Step 3.

### Initiating event and fault sequence identification

1. My expectation, informed by ONR SAP FA.2 and FA.3, is that systematic, auditable, and comprehensive fault identification should be carried out to identify faults that could give rise to a significant radiological consequence. It is also my expectation that design basis methodologies are applied to faults that have a frequency and unmitigated radiological consequence that exceeds Target 4 (FA.5). This generally means that any fault with a frequency of greater than 10-5 pa are considered for design basis analysis.
2. The RP uses the terminology ‘design basis conditions’ (DBC), and ‘design extension conditions’ (DEC) A & B to categorise plants states. The RP’s definition of DBCs is closely aligned with ONR’s definition of the design basis region. DEC-A includes beyond design basis accidents without core melt, and DEC-B covers severe accident conditions. In this section I cover DBC and DEC-A fault identification. DEC-B is covered by the severe accident analysis topic area (ref. [58]).
3. The RP has developed a methodology for the identification of initiating events which reflects the systematic process used to review the developing design (ref. [59]). The methodology employs HAZID activities (involving failure modes and effects analysis and hazard and operability (HAZOP) studies), for each system as they reach an appropriate level of maturity. The RP states the intent that these studies are then revisited as the design develops. The Rolls-Royce SMR Hazard Log (ref. [43]) presents a consolidated list of hazards, and is used to screen them from further consideration or group them for further analysis, according to their unmitigated consequence and the nature of the hazard. Given the varying level of design maturity for the plant systems the hazard log is a live document and will continue to develop with the design. As such, the RP acknowledges significant gaps in the information presented in the Hazard Log (ref. [43]) at present, and has committed to investigate potential faults arising from loss of support systems, spurious actuation of C&I systems, fuel route operations and in shutdown.
4. A list of Postulated Initiating Events (PIE) identified by the RP to date are presented in (ref. [44]), along with associated estimates of initiating event frequency (IEF). The suitability of the RP’s estimated IEFs is within the scope of the PSA assessment (ref. [60]). The criteria chosen by the RP, of including events down to 10-5 per annum (pa) in the design basis, is aligned with my expectation informed by SAP FA.5, and I am content that the RP’s approach to grouping of similar faults is appropriate and consistent with SAPs FA.6 and NS-TAST-GD-006.
5. To further investigate the completeness of the list of PIEs the RP has undertaken a comparison against other publicly available lists of PWR design basis faults, and identified a number of DBCs from these sources that were not included in the generic Rolls-Royce SMR list. For each of these fault groups the RP has noted that they need to be added in a future revision; or presented a justification for why they are not included. These justifications are generally based on differences in the design or on grounds of low consequence. I consider the comparison of the RP’s list of DBCs with others available is a benefit to the safety case and aligned with the expectations set out on fault identification in NS-TAST-GD-006, that multiple techniques should be applied to ensure completeness.
6. When a PIE is identified as being within the design basis, it is assigned a plant state categorisation of either DBC-2, DBC-3 or DBC-4. The DBC-2 and DBC-3 categories are divided to account for the RP’s differentiation between abnormal operations (DBC-2i), frequent faults (DBC-2ii and DBC-3i) and infrequent faults (DBC-3ii). These categorisations are important for identifying where ‘diverse protection’ for frequent faults may be necessary.
7. The DEC-A category comprises multiple failures, and the stated objective of the RP’s future analysis is to demonstrate that the design is sufficiently robust to ensure such events do not escalate to core melt, and that there is adequate margin to avoid cliff edge effects. It’s important to note a distinction between the RP’s approach and the international treatment of DEC-A events in SSR-2/1 and SSG-2 (refs. [34] and [35]). Whilst the international definition would include a sequence with a frequent initiating event and failure of the principal means of protection, the RP consider these sequences as DBC-4 events within the design basis. The RP’s approach aligns more closely with ONR SAPs, in that ONR expects that design basis techniques are applied down to sequence frequencies of 10-7 pa. The remaining sequences are considered within the DEC-A analysis. In my opinion, this is consistent with ONR’s expectations for beyond design basis accidents (SAPs para 638).
8. Whilst I am content the RP’s approach broadly aligns with the expectation that multiple failure and beyond design basis faults are identified, additional work is required to ensure that the RP identifies all potential DEC-A scenarios. Furthermore, these DEC-A scenarios will also require appropriate analysis in Step 3. Although not reported in Step 2, the response to RQ-01248 (ref. [61]) provides me with some confidence that the RP is planning to demonstrate that they have been appropriately considered as part of the GDA process, however insufficient detail has been presented to form a judgement on the adequacy at this time and I will seek further information in Step 3.
9. Overall, I am satisfied that the RP has presented an appropriate approach to the identification of initiating events for analysis in the E3S case which appears systematic, auditable, and comprehensive. However, at this stage in the development of the design and safety case the RP has not identified all initiating faults having the potential to lead to any person receiving a significant dose, or to a significant relocation of radioactive material, as per the intent of SAP FA.2. Nevertheless, I do not have any reason to believe that this fundamental requirement of the safety case will not be achievable in the future.
10. Therefore, in summary, whilst a significant amount of additional work is required in Step 3, I consider that the information that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.

### Fault schedule

1. SAP FA.8 sets the expectation that DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures; and that this demonstration should be summarised on a Fault Schedule.
2. The generic Rolls-Royce SMR Fault Schedule (ref. [45]) lists the postulated initiating events identified in (ref. [44]), and identifies the estimated initiating event frequency and unmitigated consequence associated with the fault. For each fault, SSCs or actions claimed in DiD levels 2, 3, 4 and 5 are identified.
3. As no radiological consequence analysis has been performed to date the unmitigated consequence is based on engineering judgement. This is generally conservative and leads to the assumption that all reactor faults lead to core melt and hence the highest consequence band in the RP’s categorisation and classification methodology (ref. [41]).
4. This information determines the required number of safety measures and the required safety category of the functions being delivered, and this is clearly presented in the fault schedule. In this way I am content that the RP has a systematic method for identifying requirements of diverse protection for frequent faults. The Fault Schedule (ref. [45]) does not explicitly state the safety classification of the safety measures delivering the safety functions, although it can be inferred they are at least of the required classification (if not higher), and this information is presented in a separate ‘safety measures module’ (ref. [62]). In my opinion the fault schedule demonstrates adequate application of the RP’s categorisation and classification methodology (ref. [41]), for the faults identified to date.
5. Lacking from the current structure of (ref. [45]) is a presentation of diversity in the detection of fault conditions for Class 1 protection systems (SAP ESS.7), which I expect to be provided by diverse sensors, trip settings and I&C platforms. The RP argues however that traceability is provided by the I&C schedule (ref. [63]) and the various Safety Measure Design Definition reports. I consider that what’s important is that this aspect of the design has been appropriately developed and is captured within the suite of documents which forms the E3S case. Therefore, whilst this complicates the ‘golden thread’ through the safety case, I am content with the RP’s approach.
6. Overall, I am satisfied that the RP has presented an appropriate approach to the development of its Fault Schedule and am content that it is likely to meet the intent of SAP FA.8 in the future. However, at this stage in the development of the design and safety case it is clear that significant elements still require populating.
7. In summary, whilst a significant amount of additional work is required in Step 3, I consider that the information that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.

### Identification of safety functional requirements

1. It is my expectation that safety functions are identified by a structured analysis in order to demonstrate the fault tolerance of the Rolls-Royce SMR. My expectation is informed by ONR SAP EKP.4.
2. In my opinion, whilst some limited safety function identification is provided in documentation supporting system design descriptions, a holistic view of safety functional decomposition is not presented. The RP has stated that the process of going from the Fault Schedule to a lower-level decomposition of safety functions is still in development, but no further information has been forthcoming. I therefore judge that my expectations, as informed by EKP.4, have not been met during Step 2. I consider the identification of safety functional requirements, and their decomposition is an area that requires further development in the RP’s safety case.
3. In summary, insufficient detail has been presented to form a judgement on the adequacy of the information and I will seek further information with regard to this residual matter in Step 3.

### Performance analysis

1. SAP FA.4 sets the expectation that design basis analysis should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures. SAPs FA.6, FA.7, NS-TAST-GD-006 and SSG-2 (ref. [35]) inform my expectation that design basis analysis be performed according to deterministic criteria to demonstrate that consequences are reduced ALARP.
2. In Step 2 the RP has submitted analysis for a preliminary set of prioritised reactor fault groups (ref. [47]). Specifically:

* Large Break Loss of Coolant Accident (LOCA).
* Intermediate Break LOCA.
* Loss of Offsite Power (LOOP) and Station Blackout (SBO)[[6]](#footnote-7).
* Main Steam Line Break (MSLB).
* Loss of Primary Flow.
* Steam Generator Tube Rupture (SGTR).
* Turbine Trip.

1. The RP decided to prioritise these fault sequences due to novelty in the design of the safety measures which protect against them, to demonstrate adequate design and sizing of key SSCs, and to demonstrate plant behaviour in response to key phenomena. As such, the analysis presented in (ref. [47]) considers (where appropriate) the effectiveness of:

* ECC - the principal (Class 1) safety measure for control of fuel temperature.
* PDHR - the significant (Class 2) means of delivering control of fuel temperature.
* Scram - the principal (Class 1) safety measure for control of reactivity.
* ASF - the significant (Class 2) means of delivering reactivity control.

1. The first issue of (ref. [47]) only covers at power fault analysis and has been carried out against the RD6 design baseline. The RD6 design baseline for the safety measures of interest is consistent with the design described in the DRP1 report (ref. [51]). The core physics data which provides initial boundary conditions is core iteration 5b (discussed in ref. [20]). Subsequent revisions of (ref. [47]) in Step 3 are planned to cover all fault groups identified by the RP, in all operating modes, and be aligned to the RP’s second Design Reference Point (DRP 2).
2. In most cases, the effectiveness of the safety measures is assessed against the CoFT and CoR safety functions. An exception to this is the SGTR fault, in which steam generator overfill is also assessed.
3. The RP does not present analysis of all figures of merit against its chosen acceptance criteria for each fault. Rather, bounding arguments are presented. For example, the RP argues that complete loss of pumped flow is bounding for most fault scenarios, for the Scram function, as the power flow mismatch is greatest. For the demonstration of the effectiveness of PDHR, the RP argues that the SBO is bounding for most faults, as it results in a sudden complete loss of active heat removal and is reliant solely upon passive systems. Where the bounding arguments are more difficult to make using qualitative reasoning alone, the RP has presented deterministic analysis for more than one fault, or highlighted areas where further work is required to determine the most limiting conditions.
4. In all analysed cases, the RP presents availability assumptions (to cover consideration of single failure and consequential losses). However, in some scenarios it is unclear which single failure has been selected, or whether it is the bounding case. For example, whilst I acknowledge that the RP has chosen to only assume one out of three trains of PDHR in all cases, it is unclear how this would be the worst single failure for the SGTR fault, where the operation of other SSC may potentially affect SG overfill. It is my expectation that the RP provide justification for the chosen single failure for each fault. Therefore, whilst I do not think this undermines the fundamental acceptability of the design, I will follow it up during Step 3.
5. In terms of consequential failure, the RP clearly presents its assumptions. The potential for consequential LOOP is discussed for all faults and the RP provides reasoning for whether this is a penalising assumption in each case. In my opinion the RP’s safety case is clear in this regard and aligns with my expectations informed by SAP FA.6.
6. The RP states there will be no maintenance of safety systems that may impact the fault analysis during powered operations (ref. [46]). However, I note that the RP’s current safety case claim related to maintenance of Class 2 systems is that it may be permitted during power operations if the Class 1 system is available. As discussed in Section ‎4.2.1, this is not aligned with my expectations for design basis analysis, and I will follow this up in Step 3.
7. For each case, the RP clearly presents the chosen acceptance criteria. As stated previously, due to bounding arguments, not all faults are analysed against all acceptance criteria or figures of merit. For example, the SBO is not analysed against DNB, as this is argued by the RP to be bounded by complete loss of pumped flow. Conversely, the loss of flow fault is not analysed against acceptance criteria for long term cooling, as the RP claims that these are bound by SBO. In all cases, I am content that the RP has chosen appropriate acceptance criteria to demonstrate the effectiveness of the safety measures.
8. I consider that the analysis presented in (ref. [47]) adequately implements the methodology described in (ref. [46]) for the subset of faults presented. In my opinion, the RP’s preliminary analysis provides confidence that the plant configuration modelled (the RD6 design baseline) is effective in delivering the fundamental safety functions and demonstrates that identified acceptance criteria are met. As such, I do not have significant concerns that the intent of FA.4, FA.6, and FA.7 may not be met in the future. However, I note that there are several areas in which the design is still developing and that it will be necessary for the RP to perform analysis of faults in shutdown modes, non-reactor faults and DEC-A analysis. These aspects require significant attention from the RP, and I will seek further information as the design and E3S case matures in Step 3.
9. In summary, although I have identified some potential shortfalls and whilst a significant amount of additional work is required in Step 3, I consider that the information submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.

### Verification and validation

1. It is ONR’s expectation that any codes used to perform deterministic analysis in support of the design basis analysis are suitably verified and validated for use. Such expectations are informed by ONR’s SAPs AV.1 to AV.8, NS-TAST-GD-042 (ref. [29]) and IAEA Specific Safety Guide SSG-2 (ref. [35]). To support my judgements in this area I commissioned a TSC to undertake a review of the RP’s strategy, methodology, application and progress with regards to developing adequate V&V evidence.
2. The RP is employing a suite of third-party computer codes for performing safety analysis to underpin its safety case in the areas of reactor physics and thermal hydraulics. The codes used by the RP for the thermal-hydraulics elements of its DBA are RELAP5-3D, VIPRE-01 and GOTHIC. In addition, there are a number of codes employed for specific applications. However, as RELAP5-3D, VIPRE-01 and GOTHIC are the main codes used to underpin the safety case claims, I have chosen to target these. A number of core physics codes are also employed, and these are considered within the Fuel and Core Assessment Report (ref. [20]).
3. The RP’s approach to V&V of these computer codes and methods is to rely heavily on existing validation where it is applicable (ref. [49]). Where important physical phenomena have the potential to be significantly affected by the Rolls-Royce SMR design, or where a code is being used for novel design applications, the RP are carrying out (or plan to carry out) further work involving a number of benchmarking activities (e.g., benchmarking against data from existing test rigs for passive systems, analytical solutions and code-to-code comparisons) and have proposed several Separate Effects Test (SET) and Integral Effects Test (IET) rigs to ultimately provide the evidence needed to underpin the validity of the suite of codes employed. However, the validation evidence provided by this additional testing will not be available during GDA. The RP’s current position with regards to demonstrating adequate V&V for its thermal-hydraulics codes and methods is summarised in (ref. [50]).
4. Although the TSC is yet to report its conclusions, regular progress meetings have been held to discuss findings. I am therefore confident that there are no significant issues arising from the TSC’s review that would undermine the fundamental approach being followed by the RP. Clearly the evidence required to underpin the V&V claims regarding the codes and methods employed for DBA needs to be further developed in the future however, and so I will seek further information in this regard in Step 3.
5. I also intend to commission a suite of independent analysis with third party computer codes, to inform our judgments in Step 3. This work will also provide additional insight with regard to the adequacy of the RP’s analysis.
6. In summary, a significant amount of additional work is required in Step 3 (and beyond) to fully validate the RP’s codes and methods for DBA. Nevertheless, I consider that the information submitted to date is consistent with UK RGP and I do not have any significant concerns, at this stage, that the RP will be able to further develop the necessary evidence for its E3S case in the future.

### Radiological consequences

1. A fundamental objective of DBA is to show that the consequences of fault sequences are ALARP (SAP FA.7) following the successful operation of identified safety measures. My judgements on whether the RP has adequately demonstrated that the consequences resulting from design basis faults are ALARP are therefore informed by the estimated dose consequences to workers and the public, and a comparison of those estimated doses with Target 4 of the SAPs.
2. I note that a methodology for producing design basis radiological consequence analysis has been produced by the RP (ref. [64]). Due to the timing of its production however, it has not been assessed in Step 2. The methodology, and the RP’s plans for producing the necessary analysis will therefore be the subject of further engagement in Step 3.
3. Moreover, whilst the methodology has been submitted, no radiological consequence analysis has been submitted at this time. However, on the basis that fuel acceptance criteria and core inventory are similar (or lower) than other light water reactors that have undergone GDA, and that the containment should retain the vast majority of any radionuclides that are released from the primary circuit, I have no fundamental concerns with the generic Rolls-Royce SMR design in this regard, at this stage.
4. In summary, insufficient detail has been presented to form a judgement on the adequacy of the RP’s radiological consequence analysis for design basis faults and I will seek further information with regard to this residual matter in Step 3.

### Implications of boron free operation

1. The Rolls-Royce SMR design does not employ boron as a means of controlling reactivity in normal operations. A design choice which is novel in civil pressurised water reactors. This decision, and the RP’s reasoning for it, is presented in a Rolls-Royce SMR Limited Boron-Free Decision Record (ref. [65]).
2. The RP’s boron free operating regime has a range of implications. The effect that this design choice has with respect to power excursion and relevant acceptance criteria in reactivity faults is of particular significance from a Fault Studies perspective.
3. In contrast to operating with boron present in the primary coolant, in which control rods are nearly fully withdrawn from the core, boron-free operation requires significant time with rods deeply inserted. As such uncontrolled withdrawal of rods may lead to significant reactivity addition. However, the RP claim that without soluble boron in the coolant, a large negative moderator temperature coefficient exists at all times, which provides inherent reactivity control in these scenarios. Indeed, core performance analysis, with core iteration 6, presented by the RP for Rod Ejection Accidents (REA) has demonstrated that the power excursion associated with ejection of a single rod may be controlled by the inherent negative moderator temperature coefficient (ref. [66]). Such events, while having very large power spikes, do not exceed peak radial averaged peak fuel enthalpy (RAPFE) criteria; and margin is demonstrated to both maximum fuel and cladding temperature criteria. I note that minimum DNB Ratio (DNBR) results indicate the potential for fuel failures in a small number of specific circumstances from 50% initial power level. Nevertheless, core design optimisations such as power dependent insertion limits are yet to be performed and I note that the current analysis with S5K employs an assembly quadrant averaged thermal hydraulics model which introduces conservatism. Future Rod Ejection Accident (REA) analysis will couple VIPRE, for subchannel thermal-hydraulics, to S5K for the analysis of DNBR, providing greater fidelity in the results, reducing conservatism and improving margin in the analysis. I therefore have confidence that acceptable DNBR margin may be demonstrated in the future, and I am content with the RP's position for Step 2.
4. Conversely, with regards to increase in heat sink faults, the strong negative moderator temperature coefficient may lead to an increase in reactor power. The RP has presented analysis of a MSLB (ref. [47]), which it argues to be bounding in this regard as it causes the largest cooldown rate and hence the largest increase in reactivity prior to Scram. The RP claims that the analysis in (ref. [47]) demonstrates margin to both minimum DNBR and maximum fuel temperature acceptance criteria which gives me confidence that the RP’s decision to remove soluble boron in normal operations does not negatively impact the faut tolerance of the plant. In addition, since a relatively higher shutdown margin is achieved by the rods alone (i.e., no dependence on boron for hold-down), the continued cooldown of the primary circuit following rod insertion does not challenge the shutdown margin. This is a benefit to the Rolls-Royce SMR. I note however that the RP identifies analysis of the limiting steam line break that the ASF can provide protection against as further work, and I consider that a demonstration this will bound all frequent faults will be required as part of that further work in Step 3.
5. In addition, I recognise there are significant benefits arising from this design choice from a Fault Studies perspective as it eliminates the possibility of boron dilution faults. This class of faults contributes 10% or more to the overall core damage frequency predicted in other PWR designs and so represents a beneficial simplification, and increased fault tolerance, of the generic Rolls-Royce SMR design.
6. In summary, I consider that the information submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence.

### Safe operating envelope

1. SAP FA.9, and NS-TAST-GD-035 (ref. [28]) set ONR's expectation that the fault analysis (together with engineering substantiation) is used in the identification of Operating Rules (OR) and hence the safe operating envelope of the plant.
2. Chapter 16 of the E3S case (ref. [9]) states that ORs are still in development through the specification of requirements in the design and safety analysis, and also that details of the operational documentation (procedures, technical specifications etc.) will be developed by the future licensee and covered in Chapter 13 in a future revision of the E3S case. Although operating limits and conditions are to be defined by the future licensee, I consider that it is still necessary for the RP to explain how the fault analysis will enable their future development.
3. Although it is not clear in the current version of the E3S case that there is (or will be) and auditable trail from the safety case to the limits and conditions embodied in the final operational documentation, information provided in response to RQ-01245 (ref. [61]) provides me with some confidence that the safe operating envelope may be appropriately defined in the future.
4. Therefore, in summary, although I consider that insufficient detail has been presented to form a judgement on the adequacy of the information at this stage, I will seek further information with regard to this residual matter as the design and E3S case matures in Step 3.

### ALARP by design

1. As discussed in Section 3, the generic Rolls-Royce SMR design provides four key safety measures for the control of reactivity (CoR) and control of fuel temperature (CoFT) at DiD level 3. These being:

* ECC – which provides the first protective safety function for loss of coolant accidents and the second protective safety function for frequent faults. ECC is the principal means of delivering the heat removal safety function and is a Class 1 safety measure.
* PDHR – which provides the first protective safety function for frequent faults and provides a significant role in delivering the heat removal safety function. PDHR is a Class 2 safety measure.
* Scram – which provides the first protective safety function for delivering control of reactivity. Scram is a Class 1 safety measure.
* ASF – which provides the second protective safety function for delivering control of reactivity and is a Class 2 safety measure.

1. Further to my sampling in the areas targeted for assessment above, I have sought to form a judgement on the adequacy of the generic Rolls-Royce SMR design in terms of reducing risks associated with operation so far as is reasonably practicable. In Step 2 I have focussed on the fundamentals of the design from a Fault Studies perspective, and so primarily considered the operational philosophy for the key protective safety measures (DiD level 3) for CoFT, and the commonality of specific SSCs between safety measures, both within and across different levels of DiD.
2. With regard to operational philosophy, I have considered the RP’s approach to providing the CoFT safety function for frequent faults. For frequent intact circuit faults (and the Small Un-isolable LOCA) the generic Rolls-Royce SMR is designed to initiate PDHR first, and then to initiate ECC if that fails. The ECC is identified as the Class 1 principal means of delivering the safety function and the PDHR is identified as the Class 2 means, providing a significant role in delivering the safety function. Whilst I consider that the generic Rolls-Royce SMR design may meet the RP’s deterministic rules and acceptance criteria in fault conditions, it is my expectation (informed by ONR SAP FA.7) that for design basis faults none of the physical barriers to prevent the escape or relocation of a significant quantity of radioactive material is breached or, if any are, then at least one barrier remains intact and without a threat to its integrity. The requirement to depressurise the primary circuit in order to enable ECC for intact circuit faults may potentially be at odds with this expectation, as I consider that the pressure and temperature transients experienced during a fault scenario represent a threat to the integrity of the fuel clad and containment. Moreover, the RP’s approach differs from other gigawatt scale PWRs, which have dedicated Class 1 protective safety systems for both intact circuit faults and LOCAs.
3. I consider that there may be reasonably practicable design modifications that could enhance the robustness of the design in this regard. Notably, the preliminary suite of plant performance analysis (ref. [47]) indicates that PDHR v1 can operate successfully with reliance solely upon SSCs that have 3-fold redundancy (the passive steam condensing system and LUHS tanks). As such, it may potentially be claimed to be Class 1 for some configurations, although I recognise that this would have implications for C&I (as per SAP ESS.7). I therefore consider that any potential plant modifications appear to be relatively straightforward to implement, with limited impact on the C&I system architecture (although I recognise that the RP has processes in place to evaluate, and govern the incorporation of, potential design changes). Whilst I consider that the RP’s current design choice represents a potential shortfall against RGP it does not undermine the fundamental acceptability of the design for Step 2. The extant version of the RP’s E3S case does not provide any justification for this aspect of the design however, and so I will continue to explore it, and any wider impacts on the generic Rolls-Royce SMR design, in Step 3.
4. Through my assessment in Step 2 it has become apparent that ASF is designed to operate with PDHR providing CoFT. ECC is compatible with Scram only and has not been substantiated to operate in conjunction with ASF. ATWS scenarios with failure of both Scram & PDHR are argued to be beyond design basis by the RP on frequency grounds. Whilst it may be the case that further failure of PDHR following an ATWS would render the sequence frequency lower than 10-7 pa, I consider there would be value in analysing this sequence on a deterministic basis, as the Class 1 ECC is the principal means of delivering CoFT, and a demonstration of no cliff edge effects may strengthen the RP’s case regarding the fault tolerance of the design. Conversely, were the analysis to show no safety margin it would support the argument for potentially increasing the reliability of the PDHR system. As discussed in section 4.2.3 additional work is required to ensure that the RP identify all potential DEC-A scenarios, and as such I will continue to explore this in Step 3.
5. ONR SAP EKP.3 sets the expectation that that there should be independence between levels of DiD, so far as is reasonably practicable, and SAP para 413 also states that safety measures should be physically separate, independent, and share no equipment or services. This is aligned with the guidance in the WENRA Reactor Harmonization Working Group (RHWG) Report Safety of new NPP designs (ref. [67]) (position 2). This expectation is a fundamental key principle and has significant implications for a reactor design. For this reason, I have targeted the independence of SSCs that constitute the key safety measures for provision of decay heat removal (specifically LUHS tanks and Refuelling Pool water volumes). Preliminary design information (refs. [52], [53] and [68]) shows that the generic Rolls-Royce SMR design shares some specific SSCs between safety measures, both within and across different levels of DiD. The RP’s ALARP Summary Report (ref. [56]), notes that the provision of dedicated LUHS for each of the PDHR and ECC safety measures was evaluated and not selected, as dedicated LUHS for each would increase the size of the plant footprint, its complexity and lead to increased build duration and cost.
6. With regards to the Refuelling Pool, the RP claims it is a massive and passive structure with highly reliable structural integrity. Any leaks are argued to be within the capacity of the HPIS recirculation pumps which would be able to maintain adequate Refuelling Pool inventory for PDHR. For potential leaks larger than the HPIS recirculation pump capacity, the RP argues the SSC would fail safe and result in containment flood up (ref. [56]). The HPIS suction line is claimed to be positioned so that it would remain submerged in such a scenario, and continue to operate.
7. Whilst these design choices do not appear to meet the intent of SAP EKP.3 and (ref. [67]), I consider that they may potentially be appropriate and lead to the most balanced design as the safety benefits derived from including separate heat sinks and in containment water volumes may be grossly disproportionate to the costs. Moreover, I note that similar sharing of massive, passive water volumes is employed by other PWR designs and so represents RGP in this particular regard. I therefore judge that this does not undermine the fundamental acceptability of the design for Step 2. Further evidence will be required to underpin the RP’s position however, and I will continue to explore this in Step 3.
8. In summary, I have identified potential shortfalls against UK RGP with regard to the classification of the SSCs that support the PDHR safety measure and the commonality of specific SSCs between safety measures. I will follow these residual matters up in Step 3.

# Conclusions

## Conclusions

1. This report presents the Step 2 Fault Studies assessment for the GDA of the Rolls-Royce SMR design. The focus of my assessment in this Step was towards the fundamental adequacy of the design and safety case. I have assessed the Tier 1 E3S chapters and relevant supporting documentation provided by Rolls-Royce SMR Limited to form my judgements. I targeted my assessment, in accordance with my assessment plan (ref. [17]), at the content of most relevance to Fault Studies against the expectations of ONR’s SAPs, TAGs and other guidance which ONR regards as RGP.
2. Based upon my assessment, I have concluded the following:

* The RP has developed a suitable set of safety analysis methodologies and principles that will enable it to deliver adequate design basis analysis to support the E3S case in the future. However, I have identified a potential shortfall against UK RGP with regards to assumptions on maintenance restrictions for Class 2 safety measures, and I will follow this up in Step 3 as a residual matter.
* The RP has developed a suitable methodology to ensure a graded approach to the categorisation of safety functions and classification of safety measures. The information that has been submitted is largely consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* The RP has presented an appropriate approach to the identification of initiating events for analysis in the E3S case which appears systematic, auditable, and comprehensive. However, at this stage in the development of the design and safety case the RP has not identified all potential initiating faults. Whilst a significant amount of additional work is required in Step 3, I consider that the information that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* The RP has presented an appropriate approach to the development of its Fault Schedule. However, at this stage in the development of the design and safety case it is clear that significant elements still require populating. Whilst additional work is required in Step 3, I consider that the information that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* The identification of safety functional requirements, and their decomposition is an area that requires further development in the RP’s safety case. Insufficient detail has been presented to form a judgement on the approach in Step 2, and I will seek further information with regard to this residual matter in Step 3.
* Whilst a significant amount of additional work is required by the RP in Step 3, I consider that the performance analysis that has been submitted to date is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* Whilst a significant amount of additional work is required by the RP in Step 3 (and beyond) to validate its DBA codes and methods, I consider that the information submitted to date is consistent with UK RGP and I do not have significant concerns, at this stage, that the RP will be able to further develop the necessary evidence for its E3S case in the future.
* Insufficient detail has been presented in Step 2 to form a judgement on the adequacy of the RP’s radiological consequence analysis for design basis faults and I will seek further information with regard to this residual matter in Step 3.
* The RP has presented suitable consideration of the implications of boron free operation, from a Fault Studies perspective. Although further core design optimisations and analysis work is necessary, I have confidence that acceptable margin may be demonstrated in relevant faults in the future, and I am content with the RP's position for Step 2.
* The identification of operating limits and conditions, and hence the adequacy of the safe operating envelope, is an area that requires further development in the RP’s safety case. Insufficient detail has been presented to form a judgement on the approach in Step 2, and I will seek further information with regard to this residual matter in Step 3.
* With regards to the operational philosophy and overall balance of the generic Rolls-Royce SMR design I have identified potential shortfalls against UK RGP. These shortfalls relate to the classification of the SSCs that support the PDHR safety measure and the commonality of specific SSCs between safety measures. I will therefore follow these residual matters up in Step 3.

1. Overall, based on my assessment to date, and subject to the provision and assessment of suitable and sufficient supporting evidence, I have not identified any fundamental safety shortfalls that could prevent ONR permissioning the construction of a power station based on the generic Rolls-Royce SMR design.

## Recommendations

1. My recommendations are as follows:

* Recommendation 1: ONR should consider the outcomes from my assessment as part of the decision to progress to Step 3 of GDA for the generic Rolls-Royce SMR design.

# References

|  |  |
| --- | --- |
| [1] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction, SMR0004294, Issue 3, May 2024. (Record ref. ONRW-2019369590-9881). |
| [2] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 2: Generic Site Characteristics, SMR0004542, Issue 3, May 2024. (Record ref. ONRW-2019369590-9883). |
| [3] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs, SMR0004589, Issue 3, May 2024. (Record ref. ONRW-2019369590-9885). |
| [4] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 4: Reactor (Fuel and Core), SMR0004210, Issue 3, May 2024. (Record ref. 2024/27297). |
| [5] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 5: Reactor Coolant System and Associated Systems, SMR0003984, Issue 3, May 2024. (Record ref. 2024/27295). |
| [6] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 6: Engineered Safety Features, SMR0003771, Issue 3, May 2024. (Record ref. ONRW-2019369590-9886). |
| [7] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 10: Steam and Power Conversion Systems, SMR0003880, Issue 3, May 2024. (Record ref. ONRW-2019369590-9917). |
| [8] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 15: Safety Analysis, SMR0003977, Issue 3, May 2024. (Record ref. ONRW-2019369590-9923). |
| [9] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Case Chapter 16: Operational Limits and Conditions, SMR0004555, Issue 3, May 2024. (Record ref. ONRW-2019369590-9922). |
| [10] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 19: Emergency Preparedness and Response, SMR0004571, Issue 3, May 2024. (Record ref. ONRW-2019369590-9909). |
| [11] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 24: ALARP Summary, SMR0004487, Issue 3, May 2024. (Record ref. ONRW-2019369590-9914). |
| [12] | ONR, Guidance on Mechanics of Assessment, NS-TAST-GD-096, Issue 1.2, December 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-096.docx. |
| [13] | ONR, Safety Assessment Principles for Nuclear Facilities (SAPs), 2014 Edition, Revision 1, January 2020. www.onr.org.uk/media/pobf24xm/saps2014.pdf. |
| [14] | ONR, Technical Assessment Guides. www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/technical-assessment-guides-tags/nuclear-safety-tags/technical-assessment-guides-tags-nuclear-safety-full-list/. |
| [15] | ONR, Guidance on the Production of Reports for Permissioning and Assessment, NS-TAST-GD-108, Issue No. 1, December 2022. (Record ref. 2022/71935). |
| [16] | ONR, New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-006, Revision 0, October 2019. www.onr.org.uk/media/pylbvfnz/onr-gda-gd-006.pdf. |
| [17] | ONR, Step 2 Fault Studies Assessment Plan for the Generic Design Assessment of the Rolls-Royce SMR, ONR-GDA-AP-22-006, Issue 1 February 2023 (Record ref. ONRW-2126615823-385). |
| [18] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 summary, ONRW-2019369590-8980, Issue No. 1, July 2024. (Record ref. ONRW-2019369590-8980). |
| [19] | Rolls-Royce SMR Limited, Rolls-Royce SMR Generic Design Assessment Scope, SMR0002183, Issue 2, January 2023. (Record ref. ONRW-2019369590-8058). |
| [20] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Fuel and Core, ONRW-2126615823-2757, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2757). |
| [21] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Chemistry, ONRW-2126615823-2874, Issue No. 1, July 2024. (Record ref. ONRW-2126615823-2874). |
| [22] | IAEA, Safety Standards. www.iaea.org. |
| [23] | IAEA, Nuclear Security series. www.iaea.org. |
| [24] | WENRA, Safety Reference Levels for Existing Reactors 2020. February 2021. WENRA. www.wenra.eu. |
| [25] | WENRA, WENRA Safety Objectives for New Nuclear Power Plants and WENRA Report on Safety of new NPP designs - RHWG position on need for revision. September 2020. www.wenra.eu. |
| [26] | ONR, Regulating duties to reduce risks to ALARP, NS-TAST-GD-005, Issue No. 12, January 2024. www.onr.org.uk/media/documents/guidance/ns-tast-gd-005.docx. |
| [27] | ONR, Design Basis Analysis, NS-TAST-GD-006 Issue 5.1, December 2022 (Record ref. https://onr.org.uk/media/documents/guidance/ns-tast-gd-006.docx). |
| [28] | ONR, Limits and Conditions for Nuclear Safety (Operating Rules), NS-TAST-GD-035 Issue 7, March 2023 (Record ref. https://onr.org.uk/media/documents/guidance/ns-tast-gd-035.docx). |
| [29] | ONR, Validation of Computer Codes and Calculation Methods, NS-TAST-GD-042 Revision 5.1, September 2023 (Record ref. https://onr.org.uk/media/documents/guidance/ns-tast-gd-042.docx). |
| [30] | ONR, The purpose, scope and content of safety cases, NS-TAST-GD-051, Issue 7.1, December 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-051.docx. |
| [31] | ONR, Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094, Revision 2, July 2019. www.onr.org.uk/media/documents/guidance/ns-tast-gd-094.pdf. |
| [32] | IAEA, Fundamental Safety Principles, Safety Standards Series No. SF-1, 2006. www.iaea.org. |
| [33] | IAEA, Safety Assessment for Facilities and Activities, General Safety Requirements No. GSR Part 4, Revision 1 2016. www.iaea.org. |
| [34] | IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1, Revision 1 2016. www.iaea.org. |
| [35] | IAEA, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2, Revision 1 2019. www.iaea.org. |
| [36] | IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide No. SSG-30, 2014. www.iaea.org. |
| [37] | IAEA, Format and Content of the Safety Analsyis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61, September 2021. www.iaea.org. |
| [38] | IAEA, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Specific Safety Guide No. SSG-70, 2022. www.iaea.org. |
| [39] | Rolls-Royce SMR Limited, RR SMR Preliminary Safety Report, SMR0001510, Issue 1, August 2022. (Record ref. 2022/51262). |
| [40] | Rolls-Royce SMR Limited, Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles, SMR0001603, Issue 1, August 2022. (Record ref. ONRW-2019369590-7775). |
| [41] | Rolls-Royce SMR Limited, Rolls-Royce SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method, SMR0006518, Issue 1, July 2023. (Record ref. ONRW-2019369590-3688). |
| [42] | Rolls-Royce SMR Limited, Rolls-Royce SMR Deterministic Safety Case - Methodologies, SMR0000531, Issue 2, January 2024. (Record ref. ONRW-2019369590-6999). |
| [43] | Rolls-Royce SMR Limited, Rolls-Royce SMR Hazard Log Report – Version 7, SMR0001317, Issue 4, January 2024. (Record ref. ONRW-2019369590-7001). |
| [44] | Rolls-Royce SMR Limited, Rolls-Royce SMR Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies, SMR0001389, Issue 4, January 2024. (Record ref. ONRW-2019369590-7003). |
| [45] | Rolls-Royce SMR Limited, Rolls-Royce SMR Fault Schedule (Version 7), SMR0004444, Issue 3, January 2024. (Record ref. ONRW-2019369590-7004). |
| [46] | Rolls-Royce SMR Limited, Reactor Plant Performance Design Basis Analysis Methodology, SMR0006250, Issue 2, November 2023. (Record ref. ONRW-2019369590-5148). |
| [47] | Rolls-Royce SMR Limited, Reactor Plant Performance Fault Study Analysis Summary, SMR0007538 Issue 1, November 2023. (Record ref. ONRW-2019369590-5147). |
| [48] | Rolls-Royce SMR Limited, RR SMR E3S Design Basis Deterministic Safety Assessment Summary, SMR0009855 Issue 1, January 2024. (Record ref. ONRW-2019369590-7000). |
| [49] | Rolls-Royce SMR Limited, Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Strategy, SMR0000601, Issue 2, June 2023. (Record ref. ONRW-2019369590-3293). |
| [50] | Rolls-Royce SMR Limited, Thermal Hydraulic Analysis Methods Verification, Validation and Uncertainty Quantification Summary, SMR0007874, Issue 1, October 2023. (Record ref. ONRW-2019369590-4856). |
| [51] | Rolls-Royce SMR Limited, Rolls-Royce SMR – GDA Design Reference Report, SMR0009043, Issue 2, April 2024. (Record ref. ONRW-2019369590-8872). |
| [52] | Rolls-Royce SMR Limited, Safety Measure Design Description for Emergency Core Cooling [JN01], SMR0000911, Issue 2, October 2023. (Record ref. ONRW-2019369590-4928). |
| [53] | Rolls-Royce SMR Limited, Safety Measure Design Description for Passive Decay Heat Removal [JN02], SMR0000624, Issue 2, October 2023. (Record ref. ONRW-2019369590-4944). |
| [54] | Rolls-Royce SMR Limited, Scram [JD01] Safety Measure Design Description, SMR0000639, Issue 2, October 2023. (Record ref. ONRW-2019369590-4931). |
| [55] | Rolls-Royce SMR Limited, Safety Measure Design Description for the Alternative Shutdown Function [JD02], SMR0000638, Issue 2, December 2023. (Record ref. ONRW-2019369590-6062). |
| [56] | Rolls-Royce SMR Limited, ALARP Summary Report, SMR0009086, Issue 1, January 2024 (Record ref. ONRW-2019369590-6729). |
| [57] | Rolls-Royce SMR Limted, Justification of Design Limits – Fuel and Core, SMR0005456, Issue 2, January 2024. (Record ref. ONRW-2019369590-6679). |
| [58] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Severe Accident Analysis, ONRW-2126615823-2780, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2780). |
| [59] | Rolls-Royce SMR Limited, Rolls-Royce SMR Hazard Identification Strategy, SMR0001228, Issue 2, July 2023. (Record ref. ONRW-2019369590-3345). |
| [60] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Probabilistic Safety Analysis, ONRW-2126615823-2692, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2692). |
| [61] | ONR, Schedule of Step 2 Regulatory Queries, April 2024. (Record ref. ONRW-2019369590-9071). |
| [62] | Rolls-Royce SMR Limited, Safety Measures Module, SMR0004917\_002, January 2024. (Record ref. ONRW-2019369590-7017). |
| [63] | Rolls-Royce SMR Limited, Rolls-Royce SMR C&I Engineering Schedule, SMR0000510, Issue 2, June 2023. (Recrod ref. ONRW-2019369590-3365). |
| [64] | Rolls-Royce SMR Limited, Design Basis Radiological Consequences Assessment Methodology, SMR0010027, Issue 1, February 2024. (Record ref. ONRW-2019369590-7709). |
| [65] | Rolls-Royce SMR Limited, PCD2 Boron-Free Decision (RI-1), EDNS01000937657, Issue 1, February 2022. (Record ref. ONRW-2019369590-3566). |
| [66] | Rolls-Royce SMR Limited, Rod Ejection Accident Methodology and Analysis, SMR0009060, Issue 1, November 2023. (Record ref. ONRW- 2019369590-6501). |
| [67] | WENRA, Safety of New NPP Designs, March 2013. www.wenra.eu. |
| [68] | Rolls-Royce SMR Limited, Safety Measure Design Description for the Containment [JM01] Safety Measure, SMR0008536, Issue 1, November 2023. (Record ref. ONRW-2019369590-5413). |
| [69] | IAEA, IAEA Nuclear Safety and Security Glossary, Terminology Used in Nuclear Safety, Nuclear Security, 2022 (Interim) Edition. www.iaea.org. |

# Appendix 1 – Relevant SAPs considered during the assessment

|  |  |
| --- | --- |
| SAP No. | SAP Title |
| FA.1 | Design basis analysis, PSA and severe accident analysis |
| FA.2 | Identification of initiating faults |
| FA.3 | Fault sequences |
| FA.4 | Fault tolerance |
| FA.5 | Initiating faults |
| FA.6 | Fault sequences |
| FA.7 | Consequences |
| FA.8 | Linking of initiating faults, fault sequences and safety measures |
| FA.9 | Further use of DBA |
| AV.1 | Theoretical models |
| AV.2 | Calculation methods |
| AV.3 | Use of data |
| AV.4 | Computer models |
| AV.5 | Documentation |
| AV.6 | Sensitivity studies |
| EKP.3 | Defence in depth |
| EKP.4 | Safety function |
| EKP.5 | Safety measures |
| ECS.1 | Safety categorisation |
| ECS.2 | Safety classification of structures, systems and components |
| EDR.1 | Failure to safety |
| EDR.2 | Redundancy, diversity and segregation |
| EDR.3 | Common cause failure |
| EDR.4 | Single failure criterion |

1. Protective safety measures sit at level 3 in the defence-in-depth (DiD) hierarchy described in SAP EKP.3 and IAEA Safety Requirements SSR2/1. [↑](#footnote-ref-2)
2. The rapid shutdown of the reactor by insertion of control rods. [↑](#footnote-ref-3)
3. The ‘first’ protective safety function refers to the DiD L3 protective safety function which is demanded first chronologically, rather than the ‘Principal’ safety function which is delivered by Class 1 SSCs. I note that NS-TAST-GD-094 recognises the ‘principal’ / ‘significant’ / ‘other’ means of delivering a safety function usually relates to the position in the hierarchy of defence in depth and, often, but by no means always, to the order in which the SSCs respond to the progression of a fault. [↑](#footnote-ref-4)
4. The ‘second’ protective safety function refers to the DiD L3 protective safety function, which is demanded second chronologically, regardless of the safety classification of the associated SSCs. [↑](#footnote-ref-5)
5. The IAEA glossary (ref. [69]) presents plant states following an accident with reference to the ‘controlled state’ and ‘safe state’, defined as:

   Controlled state - *Plant state, following an anticipated operational occurrence or accident conditions, in which fulfilment of the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.*

   Safe state - *Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time*. [↑](#footnote-ref-6)
6. A LOOP event (or ‘loss of grid’) leads to a switch to house load, or should that fail, reliance on standby AC power supplies (emergency diesel generators). In a SBO scenario, the initiation of alternative supplies has not been successful. [↑](#footnote-ref-7)