|  |
| --- |
|  |
| ONR Assessment Report  Generic Design Assessment of the Rolls-Royce SMR – Step 2 assessment of Electrical Engineering |



ONR Assessment Report

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

**Report Title**: Step 2 assessment of Electrical Engineering

**Authored by**: [Redacted]

**Report Issue No**: 1

**Document ID**: ONRW-2126615823-3090

**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 outcomes of my Electrical Engineering 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 increase 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 safety and security cases.

I targeted my assessment, in accordance with my assessment plan, at the content of most relevance to Electrical Engineering against the expectations of ONR’s Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and other guidance which ONR regards as relevant good practice.

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

* Development of Safety Case for Electrical Engineering.
* Electrical Power System Architecture.
* Through Life Management.
* Support to Human Operations.
* Smart Device Strategy.
* Categorisation of safety functions and classification of systems, structures and components.
* Heating Ventilation and Air Conditioning of Electrical Equipment.
* Use of Variable Frequency Drives.
* Grid Code Compliance.

Based upon my assessment, I have concluded the following:

* Use of direct current (DC) power to initiate passive safety measures for Class 1 equipment important to safety has the potential to overcome the need for Class 1 standby AC onsite power sources.
* Architecture of the electrical systems, with redundant divisions fed by multiple offsite and onsite power sources, provides the basis of a design which should be capable of meeting international guidance and ONR’s expectations for redundancy and defence-in-depth.
* The clarity of the safety case needs to be improved to comprehensively identify the risks associated with the electrical system and demonstrate how the design reduces those risks so far as is reasonably practicable.
* The autonomy times for onsite power sources shall be demonstrated to be consistent with the expectations of a design basis loss of offsite power event.
* The heating, ventilation and air conditioning (HVAC) system design shall appropriately consider the needs of the electrical system.

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

AC Alternating Current

ALARP As low as is reasonably practicable

BAT Best Available Technology

BD High Voltage Essential AC Standby Supply System

BL Low Voltage Essential AC Alternate Supply System

BK Low Voltage Essential AC Standby Supply System

BQ Low Voltage Uninterruptible DC Supply System for Safety Services

BP Low Voltage Uninterruptible DC Supply System

BSI British Standards Institution

C&I Control and Instrumentation

CAE Claims, Arguments and Evidence

DBC Design Basis Condition

DC Direct Current

DOORS Dynamic Object-Oriented Requirements System

DPS Diverse Protection System

DR3 Definition Review 3

E3S Environment, Safety, Security and Safeguards

EIMT Examination, Inspection, Maintenance and Testing

EMIT Examination, Maintenance, Inspections and Testing

GB Great Britain

GDA Generic Design Assessment

HAZOP Hazard and Operability Anal

HVAC Heating, Ventilation and Air Conditioning

IAEA International Atomic Energy Agency

KL HVAC Systems Serving Controlled Areas and Uncontrolled Areas of the Reactor Island

LOOP Loss of Offsite Power

NG National Grid

NPP Nuclear Power Plants

NRW Natural Resources Wales

Ofgem Office for Gas and Electricity Markets

ONR Office for Nuclear Regulation

PWR Pressurised Water Reactor

RCP Reactor Coolant Pump

RO Regulatory Observation

RP Requesting Party

RPS Reactor Protection System

RQ Regulatory Query

SAP Safety Assessment Principle(s)

SBO Station Blackout

SMR Small Modular Reactor

SSC Structure, System and Component

TAG Technical Assessment Guide(s) (ONR)

TLACP Total Loss of AC Power

UPS Uninterruptable Power Supply

VFD Variable Frequency Drive

WENRA Western European Nuclear Regulators’ Association

Contents

[Executive Summary 3](#_Toc170205649)

[List of Abbreviations 5](#_Toc170205650)

[1. Introduction 8](#_Toc170205651)

[2. Assessment standards and interfaces 11](#_Toc170205652)

[3. Requesting party’s submission 14](#_Toc170205653)

[4. ONR assessment 22](#_Toc170205654)

[5. Conclusions 39](#_Toc170205655)

[References 41](#_Toc170205656)

[Appendix 1 – Relevant ONR SAPs considered during the assessment 46](#_Toc170205657)

# Introduction

1. This report presents the outcomes of my Electrical Engineering 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 (refs [1], [2], [3], [4], [5] and [6]) 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. [7]). The ONR Safety Assessment Principles (SAPs) (ref. [8]), together with supporting Technical Assessment Guides (TAGs), have been used as the basis for this assessment.
3. This is a Major report (refer to NS-TAST-GD-108 (ref. [9])).

## Background

1. The ONR’s GDA process (ref. [10]) 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 Electrical Engineering (ref. [11]). 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. [12]).

## 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. [13]). Rolls-Royce SMR Limited has indicated the intention to complete a three step GDA, with the objective of receiving a Design Acceptance Confirmation 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 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 have therefore not been considered in this assessment:

* Heating Ventilation and Air Conditioning of Diesel Houses.
* Rating and Capacity of Electrical Systems.

1. I do not consider this a significant concern at Step 2 but will expect the RP to set out the claims, design and substantiation of these aspects as the design is developed for Step 3.
2. As set out in (ref. [11]), my assessment has considered the following aspects:

* Electrical system safety case.
* Electrical system architecture.
* Through life management.
* Support to human operations.
* Smart device strategy.
* Categorisation of safety functions and classification of electrical systems.
* Demonstration of risk being reduced as low as is reasonably practicable (ALARP) as applied by the RP to the design of electrical systems.

1. I have also considered the following aspects, which from discussion with the RP, I considered warranted consideration during this step:

* Heating Ventilation and Air Conditioning of Electrical Equipment.
* Use of Variable Frequency Drives.
* Grid Code Compliance .

# 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. [8]) 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 GDA Step 2 assessment of the Rolls-Royce SMR.
2. The International Atomic Energy Agency (IAEA) safety standards and nuclear security series 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. [14]), which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors (ref. [15]).
4. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the TAGs. The TAGs provide the principal means for assessing the electrical engineering aspects in practice.

### Safety Assessment Principles (SAPs)

1. The key SAPs applied within my assessment are EKP.3, EDR.2, EDR.3, EDR.4, ECS.2, ESS.8, and EMT.1.
2. 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-003 – Safety Systems (ref. [16]).
* NS-TAST-GD-019 – Essential Systems (ref. [17]).
* NS-TAST-GD-094 – Categorisation of Safety Functions and Classification of Structures, Systems and Components (ref. [18]).
* NS-TAST-GD-096 – Guidance on Mechanics of Assessment (ref. [7]).

### National and international standards and guidance

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

* IAEA, Safety of Nuclear Power Plants: Design SSR 2/1 Rev.1 (ref. [19]).
* IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide No. SSG-30 (ref. [20]).
* IAEA, Design of Electrical Power Systems for Nuclear Power Plants, Specific Safety Guide No. SSG-34 (ref. [21]).
* IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61 (ref. [22]).
* IAEA, Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants, Specific Safety Guide No. SSG-62 (ref. [23]).
* IAEA, Design Provisions for Withstanding Station Blackout at Nuclear Power Plants, IAEA-TECDOC-1770 (ref. [24]).
* BSI, Nuclear Power Plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems, BS EN IEC 61226 (ref. [25]).
* BSI, Nuclear Power Plants – Electrical power systems – General requirements, BS EN IEC 63046 (ref. [26]).

## Integration with other assessment topics

1. I worked closely with other topics as part of my electrical engineering 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:

* Fault Studies, Control and Instrumentation, Mechanical Engineering – To ensure a consistent assessment of the approach to categorisation and classification of equipment important to safety.
* External and Internal Hazards, Fault Studies and Mechanical Engineering – To ensure a consistent assessment of the approach to management of room temperatures to extreme environmental conditions.

## Use of technical support contractors

1. During GDA Step 2, I have not used any Technical Support Contractors to support my assessment of the Topic aspects of the Rolls-Royce SMR.

# Requesting party’s submission

1. Rolls-Royce SMR Limited submitted a series of E3S case 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 electrical engineering. It also identifies the documents submitted by the RP which have formed the basis of my electrical engineering assessment of the Rolls-Royce SMR.

## 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 the 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 holding fuel assemblies, Steam Generators, 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. In developing the design, the RP has focused on using passive safety measures to deliver the necessary safety functions. Whilst the use of passive systems can reduce the safety claims on support systems such as standby AC power sources, they can increase the importance of battery-backed electrical systems to initiate, control and monitor these measures over a protracted period of time. This aspect has formed a significant element of my assessment of the architecture during Step 2.

## E3S case approach and structure

1. Rolls-Royce SMR Limited has chosen to develop the 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 Claims, Argument and Evidence (CAE) structure with the highest-level claims being derived from the RP’s own E3S case principles. The highest level of the three tiers is the RP’s Tier 1 E3S case chapters, with the lower tiers providing more detailed arguments and evidence. This is illustrated in Figure 1.

****

**Figure 1: 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. [22]), supplemented to include UK specific expectations and expanded to include the other E3S purposes.

## Summary of the requesting party’s E3S case for Electrical Engineering

1. The aspects covered by the Rolls-Royce SMR safety case in the area of electrical engineering that are considered within this Step 2 assessment can be broadly grouped under nine headings which are summarised as follows:

### Development of safety case for Electrical Engineering

1. The primary entry point to the safety case for electrical engineering is through Chapter 8 of the E3S Case (ref. [5]).
2. This sets out that the overall approach to CAE in this topic area and the set of E3S claims to achieve the E3S fundamental objective, which is described in E3S Case Chapter 1: Introduction (ref. [1]). (Ref. [5]) then sets out the specific topic level claim:

* Claim 8: Electrical Power Systems are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with secure by design and safeguards by design.

1. It decomposes this claim into a sub-claims, arguments and evidence structure through an E3S Case Route Map (ref. [27]). Given the evolving nature of the E3S Case alongside the maturing design, the RP notes that the underpinning arguments and evidence may still be developed in future design stages, but the trajectory of this information, where possible, is also illustrated in the route map.
2. It further states that “A proportionate summary of the arguments and evidence from lower tier information, available at the current design stage, is presented within the chapter”. It sets out the key codes, standards and UK regulations that the RP considers are applicable to the development of the electrical system.
3. The chapter is based on the development of the design, corresponding to the RP’s Design Reference Point 1 (DRP) (ref. [28]). The establishment of this DRP introduces change control for the design that is to be considered as part of GDA.
4. Within (ref. [5]), the safety functions to be delivered by each Structure, System and Component (SSC) are presented, with the assignment of safety categorised functional requirements to achieve them. No functional requirements for environment, security and safeguards are placed onto SSCs within the Electrical Power Systems. The design definition presented is based on the design maturity of each respective SSC.
5. The RP has identified that a significant step in the maturity of each system within the design will be attained when reaching a project milestone, Definition Review 3 (DR3). At this point, it is claimed each system will be underpinned by evidence to support the design architecture and sizing. It is expected that this milestone will be reached for the main safety electrical system during 2024.
6. The System Design Description for the Electrical Systems (ref. [29]), which is the primary reference to (ref. [5]) describes each electrical system that is within the scope of the GDA, highlighting its operation, its role in supporting safety functions, as well how it aligns with the IAEA expectations of defence-in-depth.

### Alternating Current power system architecture

1. The Alternating Current (AC) Power System consists of a number of different sub-systems, which according to (ref. [5]) provide:

* Connection to Grid Transmission System to import and export power to/from an external grid which provides normal onsite power for Design Basis Conditions (DBC-1 and DBC-2)
* Standby AC Power Supply which provides backup power through two redundant divisions to SSCs during DBC-3i Loss of Offsite Power (LOOP) fault conditions.
* Alternate AC Power Supply which provides long term backup power through two redundant divisions to SSCs during DBC-3ii Loss of Main Line of Protection and DBC-4 Station Blackout (SBO) fault conditions.

### Direct Current power system architecture

1. The Direct Current (DC) Power System consists of a number of different sub-systems, which according to (ref. [5]) provide:

* Uninterruptible supplies, supported by batteries, and including inverters to provide uninterruptible AC supplies to SSCs demanded during LOOP and SBO fault conditions, as well as other essential equipment such as fire alarms and radiation monitors.
* These vary in autonomy time from 2 hours where they provide supply interruption measures to Class 3 duty systems, through 24 hours for the Class 1 Diverse Protection System (DPS) and Class 2 Reactor Protection System (RPS) to 72 hours for the Class 3 accident monitoring systems.

### Through life management

1. The E3S Case Chapter 3 (ref. [2]) sets out the basic design principles that are to be applied to the design. The associated E3S Case Route Map (ref. [27]) sets the following sub-claim:

* An overarching approach to EMIT [Examination, Maintenance, Inspection and Testing] is defined to ensure SSCs can deliver E3S requirements through life

1. This sub-claim makes reference to the RP’s EMIT Strategy (ref. [30]) which it is stated sets the ‘framework for the full lifecycle of EMIT in the design phase, including drivers, derivation, documentation, verification, and design for EMIT activities”.
2. A dedicated claim in the E3S Case Chapter 8 (ref. [5]) sets out that:

* Verification of the Electrical Power Systems system is preserved through its operational life

1. At this time, this links back to the overall strategy set out in (ref. [30]).

### Approach to Smart Devices

1. The RP strategy for the use of smart devices is identified in the E3S Case Chapter 8 (ref. [5]), which references the SMR Electrical Protection Philosophy and Smart Devices (ref. [31]). (Ref. [31]) sets out how the management and qualification of smart devices will be managed by the RP Control and Instrumentation (C&I) team through a process set out in E3S Case Chapter 7 (ref. [4]).
2. (Ref. [31]) notes that “Most electrical protection relays available on the market are multifunction programmable relays which are classed as smart devices. There are limited options when it comes to analogue protection devices for certain protection functions and therefore this must be considered as part of the electrical protection philosophy”. It identifies likely electrical equipment which may be controlled or include smart devices and notes that whilst a final decision cannot be taken until the final detailed design/procurement stages, it notes “It is likely that these smart devices will be used for Class 3 and Class 2 systems. The use of smart devices on Class 1 systems is still under review”.

### Categorisation of safety functions and classification of systems, structures and components

1. The E3S and Safeguards Categorisation and Classification Methodology (ref. [32]) sets out how the classification of the electrical systems shall be aligned to the classification of the systems they support and according to the categorised safety functions they perform.
2. (Ref. [32]) sets out a refinement to this process in that a system providing a supporting function to a Category A or B function after 24 hours can be reduced by one category to Category B or C, respectively, and after 72 hours can be further reduced for the Category A function to Category C.
3. The E3S Case Chapter 8 (ref. [5]) and Electrical Design Rules (ref. [33]) sets out the generic rules that the RP will apply to all systems. Included within this are specific rules for segregation and separation which aim to ensure independence between systems of different classifications. This includes the requirement for isolation devices between systems of different classifications and for these to be classified consistent with the higher classified system.

### Heating Ventilation and Air Conditioning of electrical equipment

1. The E3S Case Chapter 8 (ref. [5]) and System Design Description for Electrical Systems (ref. [29]) identifies the various electrical systems which interface with the Heating, Ventilation and Air Conditioning (HVAC) systems to ensure components are operated in a controlled environment, noting that the detail of these interfaces are under development.
2. The System Design Description for the HVAC Systems Serving Controlled Areas and Uncontrolled Areas of the Reactor Island (KL) (ref. [34]) provides the system definition for the HVAC system which maintains air quality and conditions for both processes and occupants of the areas where the main electrical distribution equipment is to be located.
3. (Ref. [34]) sets out how the systems which support the areas within the reactor island containing electrical equipment will be unclassified, although electrical rooms with safety classified electrical equipment will be maintained by local cooling units of a matching classification.

### Use of Variable Frequency Drives

1. The Key Single Line Diagram identifies the use of Variable Frequency Drives (VFD) to support a number of plant equipment, including reactor coolant pumps and main feedwater pumps.
2. E3S Case Chapter 8 (ref. [5]) identifies that where VFD are to be used, they are considered as part of their associated process system, rather than part of the electrical distribution system. Their case is therefore within the respective process chapter.
3. E3S Case Chapter 5 (ref. [3]) relating to the RCPs currently includes a single line on the subject that states “During Operating Mode 2 (Start-Up), the RCPs employ a Variable Frequency Drive (VFD) to vary pump power as required, prior to transitioning to direct drive.” The VFD is therefore used to manage the current and shaft torque during start-up rather than the flow during operation.
4. Whilst E3S Case Chapter 10 (ref. [6]) makes no reference to the use of VFD to control the main feedwater pumps, the RP has identified in response to an RQ (ref. [35]), that such drives are to be used to manage the flow rate.

### Grid Code compliance

1. The ability to connect the nuclear power plant to the Great Britain (GB) transmission system is important to ensure not only that it can commercially export electrical power but also so that under normal conditions, it can receive electrical power to support safety systems. To enable this, it has to meet a number of connection conditions set out in the Grid Code (ref. [36]) as set out by the GB Transmission System Operator. Whilst legal vires for compliance with the Grid Code sit with the Office for Gas and Electricity Markets (Ofgem), the offsite electrical supply is generally the preferred power source during fault conditions and, therefore, it is important to have confidence that the design can be connected to the transmission system without impacting nuclear safety.
2. The E3S Case Route Map (ref. [27]) identifies the need through a claim for the design to meet relevant codes and standards and specifically references a National Grid (NG) Grid Code Compliance Strategy (ref. [37]). This document sets out how the RP intends to capture the individual technical code requirements through transverse requirements stored in the RP’s engineering requirements management system (known as DOORS), ensuring that the detailed design then adheres to these requirements and is ultimately demonstrated to be compliant through design verification.

### Demonstration of an ALARP design

1. The E3S Case Chapter 8 (ref. [5]) sets out through the high level Claim 8 that the “Electrical Power Systems are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with secure by design and safeguards by design”.
2. (Ref. [5]) sets out that through the design of SSCs in line with the RP’s own engineering processes, alignment to relevant good practice, use of operational experience, use of appropriate codes and standards and down-selection of options based on assessment process that considers relevant safety, security, environmental and safeguards criteria, the RP is working towards a final design that will demonstrate that safety risks are reduced ALARP.

## Basis of assessment: requesting party’s documentation

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

* E3S Case Chapter 8 – Electrical (ref. [5]).
* E3S Case Route Map (ref. [27]).
* Electrical Design Rules (ref. [33]).
* SMR Electrical Protection Philosophy and Smart Devices (ref. [31]).
* National Grid (NG) Grid Code Compliance Strategy (ref. [37]).
* Requirement Specifications (refs [38], [39], and [40]).
* Rolls-Royce SMR Generic Design Assessment Scope (ref. [13]).

# ONR assessment

## Assessment strategy

1. Based on the aspects identified in section 1.2, above, and set out in my assessment plan (ref. [11]), I have sampled the RP’s submissions identified in section 3.4, above, to gain confidence that the RP is developing a robust safety case based on fundamental claims supported by evidence, that will meet the expectations set out in the ONR SAPs and are consistent with international guidance. During this step, my assessment has focused on seeking assurance on the development of a robust safety case structure supported by sound design principles, which if applied, should ensure a strong design that can be demonstrated by evidence during Step 3.
2. My assessment has involved regular engagement with the RP’s electrical engineering specialists. This has included 15 progress meetings at the time of writing of this report.
3. During my GDA Step 2 assessment, I have identified areas in the requesting party’s submissions or strategy which have required clarification. Consistent with ONR’s Guidance to Request Parties (ref. [10]), I have raised a series of Regulatory Queries (RQ) in these areas. At the time of writing this assessment report, I have raised 12 RQs (ref. [35]) to facilitate my assessment.
4. In addition, I have taken into consideration the work being undertaken by the RP in the resolution of Regulatory Observation (RO) RO-RRSMR-001 (ref. [41]).
5. The details of my Step 2 assessment of the E3S case of the RR SMR design in the area of electrical engineering, including the conclusions I have reached, are presented in the following sub-sections of this report. This includes items that I have identified require follow-up during Step 3 of the GDA.

## Assessment

### Development of safety case for Electrical Engineering

1. The high level chapter claim for electrical engineering presented in E3S Case Chapter 8 (ref. [5]) states that:

* Claim 8: Electrical Power Systems are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with Secure-by-Design and Safeguards-by-Design.

1. The E3S Case Route Map (ref. [27]) breaks this claim down through a series of sub-claims relating to functional and non-functional requirements with the purpose of demonstrating that the correct and appropriate requirements have been developed to support the safety functions required of it. A further leg of the claims structure sets out how the electrical power system implements all these requirements, thereby aiming to demonstrate that the designed system is robust. All the RP submissions considered in this Step 2 assessment are identified in the claims structure set out in (refs [5] and [27]).
2. The claims structure refers out to a series of individual requirements that the RP manages through a computer-based relational database (known as DOORS). The RP has provided extracts of this database for each of the principal electrical systems identified in (ref. [5]). I sampled these documents (refs [38] and [42]) and am satisfied that individual requirements within it can be considered a proxy for a sub-claim on the system, as shown in the following quotes:

* The High Voltage AC Essential Supply Systems (BD) Backup power sources shall be capable of auto-synchronise.
* The High Voltage AC Essential Supply Systems (BD) Backup power sources shall be capable of auto-starting.
* The Low Voltage Electrical Supply System 2 for Safety Services (BL) shall have capability to select one power source only from the two power sources below: - Alternate AC Power Source / Mobile Power Source. - BK System.

1. In addition, the RP has identified an approach which uses transverse requirements (ref. [33]) to capture provisions that need to apply to multiple systems or that span multiple systems. This includes aspects such as single failure criterion, common cause failure or protection philosophy. These groups are then applied to each of the relevant electrical systems. At this point in the design development, this mapping is not yet complete but the RP has indicated that this will be complete by the end of Step 3 where the intention will be either to demonstrate how the design will meet the requirement or where it is not applicable, justify why.
2. From a review of the individual requirements, I consider that they provide a consistent base aligned to the ONR SAPs relating to the deterministic principles of EKP.3, ECS.2, EDR.2, EDR.3 and EDR.4. However, it is not clear from the current safety case structure how the RP intends to provide the traceability with evidence from the individual requirements to each of the relevant systems and then demonstrate how the system has been designed to meet that requirement. It is also not currently apparent how these claims will work together to demonstrate a robust holistic design, since there is no hierarchical case structure at present to consider those safety case ‘claim themes’ which span systems. Concerns with the clarity and development of the safety case structure have been recognised across the project and are captured in cross-discipline Regulatory Observation RO-RRSMR-001 (ref. [41]), which I will continue to support into GDA Step 3.
3. I consider the submitted Design Reference Point (ref. [28]), which sets out the basis for the design, is consistent with the information provided in (ref. [5]) and its supporting references. I consider it provides a sound basis on which the RP can control the design that is assessed as part of GDA during Step 3.
4. In summary, I consider that through the individual system Requirements Specifications and the Transverse Requirements, the RP is identifying the principal targets to develop a robust deterministic safety case and has the appropriate overall objective. However at this time, it is not clear how the RP will demonstrate that all of the individual requirements are reflected in the design and ultimately in the constructed plant, or how it will be demonstrated that they all work together to provide a holistic case. During GDA Step 2, I have sought clarity on how the RP intends to achieve this and have been advised that as the design develops, the intention is to develop a mechanism to demonstrate both the holistic case and the individual requirements during GDA Step 3.
5. I consider that the RP will need to develop a more specific claims structure which demonstrates how the systems individually, and collectively, meet the deterministic and probabilistic expectations for the RR SMR design, and show how the evidence that will be produced in GDA Step 3 will substantiate this. I consider that the work being done in response to Regulatory Observation RO-RRSMR-001 will make a significant contribution to achieving this and will follow this up during GDA Step 3.

### Alternating Current (AC) power system architecture

1. I have assessed the AC power system architecture of the design based on information provided in E3S Case Chapter 8 (ref. [5]), System Design Description (ref. [29]) and electrical single line diagrams (refs [43] and [44]), responses to RQs (ref. [35]) and supported by discussions with the RP during progress meetings.
2. Noting that the design is evolving, and the detailed substantiation is not yet available, I have focused my assessment on establishing whether the basic architecture supports:

* Connection of offsite power supplies;
* Onsite power supplies;
* Divisional segregation of the AC power systems;
* Application of categorisation and classification principles to the electrical systems;
* Resilience to common cause failure; and
* Impact of operating modes and maintenance on the system.

1. As a result, I have considered the following SAPs (ref. [8]):

* EKP.3 (Defence in depth);
* EDR.2 (Redundancy, diversity and segregation);
* EDR.3 (Common cause failure);
* EDR.4 (Single failure criterion); and
* ESS.8 (Automatic initiation).

1. I have considered the WENRA Safety of new NPP designs (ref. [15]), IAEA Specific Safety Guide SSG-34 (ref. [21]), IAEA Technical Document on Design Provisions for Withstanding Station Blackout (ref. [24]) as well as the ONR TAGs on Safety Systems (ref. [16]) and Essential Services (ref. [17]) to support my judgements.
2. However, as noted in the E3S Case Chapter 8 (ref. [5]) and the introduction to the Requirements Specifications (ref. [38]), the information presented at this time is based on the design definition at the end of Preliminary Concept Definition (PCD), which is an interim design stage and that as the design develops the RP will generate further evidence including the definition of safety-categorised functional and non-functional requirements. A significant step in the RP’s design process is the ‘DR3’ milestone, when detailed substantiation evidence will be available. The RP expects to reach this milestone for each of the electrical systems during 2024.
3. However, despite this current level of design immaturity, based on the evidence submitted, I consider that the AC power system architecture of the design is consistent with that identified in (ref. [21]), reflecting the provision of two offsite transmission system connections supplying three main electrical switchboards. These two offsite connections provide a significant role in reducing the claims on the onsite power sources and the risk of a LOOP event. At this time, the RP has not developed the arrangements for switchover. During GDA Step 3, I will expect the RP to demonstrate how it is intended to manage the connection of these two supplies and demonstrate that the timing of any switchover is consistent with the starting of any onsite generators or deployment of any passive safety measures.
4. The onsite safety power supply system consists of two independent electrical trains, each of which is backed up by an auto-starting high-voltage Standby AC Diesel Generator. This is consistent with the ‘passive’ strategy of the design to use DC backed supplies to support passive safety measures as the main line of defence, with two independent ‘active’ trains providing a diverse function.
5. The proposal for 72 hours autonomy for the Standby AC Diesel Generator appears inconsistent with IAEA guidance (refs [21] and [24]) as well as previous GDAs where an autonomy time of 168 hours has been proposed. In addition, changes over the last decade to the generation mix of the GB energy market mean that a nationwide blackout may take up to 5 days to fully recover from (ref. [45]). I have engaged with the RP during Step 2 and they have advised that the figure is subject to review as part of the ‘DR3’ milestone. I will consider this further as part of my assessment during Step 3.
6. The RP states that ‘temporary connections between redundant divisions shall be made during shutdown’. There is a balance to be made between maintaining independence of divisions and maximising the availability of systems of lower importance during maintenance of the electrical distribution systems that normally supply them. Whilst I consider the intent to provide such connections only during shutdown reasonable, I shall, during GDA Step 3, review how it is intended this will be realised and seek confidence through the E3S case that the risks of a resulting multi-division failure are reduced so far as is reasonably practicable, thereby meeting the expectations of ONR SAP EDR 2.
7. The design includes the provision of additional low-voltage Standby AC Diesel Generators. I was concerned that there could be a dependency between these and the high-voltage diesel generators, which if either failed could result in the unsuccessful delivery of a safety function. In response to an RQ (ref. [35]), the RP has advised that the intent is that the low-voltage diesel generators will be used for asset protection and the provision of Class 3 safety functions away from the reactor island. As such, the RP has stated there will be no safety functions which are dependent on the availability of both types of diesel generators. I consider this another positive statement, which is in line with ONR SAP EDR.2, and will seek assurance during GDA Step 3 that this continues to be the case as the design matures and this requirement is reflected in the safety case.
8. The design includes the provision of two manually started low-voltage Alternate AC Diesel Generators, which provide power to recharge the batteries that provide power to the Class 1 reactor protection system and supports systems that may be required in response to an SBO situation. The RP has stated that these will be diverse to the Standby AC Diesel Generators. Whilst there are requirements specifications that there will be diversity and segregation for the respective systems, it is not clear with the current design maturity how it is intended to achieve these, as discussed in Paragraph ‎79, above. During GDA Step 3, I will seek evidence that substantiates these individual claims to gain confidence that when considering the electrical system holistically the RP is appropriately demonstrating the robustness of the design to the deterministic principles such as common cause failure, as well as the consideration of the time available to start the diesel generator and therefore consideration of ONR SAPs EDR.3 and ESS.8.
9. Based on the outcome of my GDA Step 2 assessment of the AC power system architecture, I have concluded that the fundamental architecture appears to be robust and consistent with ONR SAPs EKP.3, EDR.2, EDR.3, EDR.4, ESS.8, IAEA Safety Guide SSG-34, and WENRA guidance (ref. [15]). At this time, the evidence to substantiate this has not been presented and I will consider this further in GDA Step 3.

### Direct Current (DC) power system architecture

1. I have assessed the DC power system architecture of the design based on information provided in E3S Case Chapter 8 (ref. [5]), System Design Description (ref. [29]) and electrical single line diagrams (refs [44] and [43]), responses to RQs (ref. [35]) and supported by discussions with the RP during progress meetings.
2. Noting that the design is evolving and the detailed substantiation is not yet available, I have focused my assessment on establishing whether the basic architecture supports:

* Appropriate battery autonomy times;
* Divisional segregation of the DC systems;
* Resilience to LOOP and SBO situations;
* Ability to support reactor protection systems;
* Application of categorisation and classification principles to the electrical systems;
* Resilience to common cause failure; and
* Effect of operating modes and maintenance on the system.

1. As a result, I have considered the following SAPs:

* EKP.3 (Defence in depth);
* EDR.2 (Redundancy, diversity and segregation);
* EDR.3 (Common cause failure);
* EDR.4 (Single failure criterion); and
* ESS.8 (Automatic initiation).

1. I have considered the IAEA Specific Safety Guide SSG-34 (ref. [21]) as well as the ONR TAGs on Safety Systems (ref. [16]) and Essential Services (ref. [17]) to support my judgements.
2. The design utilises DC systems to support safety systems for the following reasons:

* To provide electrical power which are required during normal operation and for which a short disturbance in supplies could initiate a reactor trip.
* To provide electrical power to safety systems until the Standby AC Power Diesel Generators are started.
* To provide electrical power to reconfigure fluid systems and then monitor the conditions when the passive safety measures are to be initiated.

1. This final aspect is driven by a strategy for the design to utilise passive safety measures wherever practicable, and certainly for systems those of the highest Class 1 safety level. However, in reality few systems can be completely passive and whilst after realignment an appropriately designed safety system can continue to function through natural circulation or gravity to deliver its safety function, it typically requires an energy source to detect an event has occurred, reconfigure the system from normal operation through the operation of valves and then require on-going monitoring to ensure the plant achieves a controlled and safe state. As reflected in (ref. [5]), this requires electrical supplies. The design aims to achieve this without the need for diesel generators, utilising DC batteries.
2. As presented in (ref. [5]), the System Design Description (ref. [29]) and the associated single line diagrams (refs [43] and [44]), the RP has selected an architecture which provides individual DC power systems that support individual safety systems with autonomy times that it is claimed will be consistent with the mission time of that system and with a strategy to be able to recharge the batteries in the longer term from dedicated diesel generators. It is noted that the DC Power Systems all utilise a charger, battery and inverter arrangement to provide DC power as well as non-interruptible AC power to systems that they support. The exception is the Class 1 Diverse Protection System, where the design does not include inverters and the C&I systems and associated SSCs, such as valves, are to be powered by DC. I consider this latter approach should reduce the points of failure and increase the overall reliability of the system.
3. The use of four redundant DC divisions to support the Class 1 DPS and three redundant uninterruptable power supplies (UPS) divisions to support the Class 2 RPS is consistent with the design redundancy of the two respective C&I systems. Whilst the RP has set out independence requirements in the Requirements Specifications between divisions and between the RPS and DPS, meeting the intent of the ONR SAPs considered in this section, it is not clear how the RP intends to achieve this. I will consider the evidence to substantiate this as part of my GDA Step 3 assessment.
4. The RP design sets out autonomy times of 1 hour for Class 3 systems which provide voltage disturbance and short power supply disturbance protection but are not necessary for long term safety of the plant; 24 hours for the reactor protection systems; whilst accident monitoring systems are supported by systems capable of 72 hours. I consider these durations are in line with expectations from other reactor designs (ref. [46]) and international guidance (ref. [24]) but during GDA Step 3 will seek confidence that these times are consistent with the mission times for the SSCs they support and the connection time for any backup generators that are to be used to recharge the batteries.
5. The RP design currently includes the use of two parallel batteries and two chargers per DC system in a division. Each battery is sized to provide 50% of the total energy capacity required by the safety case, whilst it is claimed that each charger will be sized to supply its respective system and charge both batteries simultaneously. The RP has advised that the intention is not to declare a system available when only one of the batteries in a system is available. It is currently not clear the benefit of this arrangement, given the potential lower reliability of the system due to the increased number of failure points. I will consider the evidence that analyses and substantiates the system sizing and this architectural approach during GDA Step 3.
6. In summary, based on the outcome of my GDA Step 2 assessment of the DC power system architecture, I have concluded that the fundamental architecture appears to be robust and consistent with ONR SAPs EKP.3, EDR.2, EDR.3, EDR.4, ESS.8 and IAEA Safety Guide SSG-34. At this time, the evidence to substantiate this has not been presented and I will seek further information in GDA Step 3.

### Through life management

1. It is important the electrical system is not only designed to deliver its safety functions but also constructed in a way that enables it to be operated, maintained and, where necessary, replaced throughout the life of the facility.
2. Noting the design is evolving, I have focused my assessment on whether the RP has established fundamental expectations for the design life of the plant and is considering ageing management and Examination, Inspection, Maintenance and Testing (EIMT) as part of the design development.
3. In my assessment, I have considered the following SAPs:

* EMT.1 (Identification of requirements), and
* EAD.1 (Safe working life).

1. The RP’s EMIT Strategy (ref. [30]) sets the reason and purpose for undertaking EIMT as part of assuring SSC reliability and ageing management of SSCs, identifying the types of techniques that could be employed as the design develops. The strategy draws on good practice approaches, such as the Institute of Nuclear Power Operations AP-913 process, or more generally reliability centred maintenance, although at this stage of the design, makes no specific commitment to implement any detailed aspects of such an approach.
2. In the System Description (ref. [29]), the RP sets out how the design of the electrical systems needs to support the installation, commission, EIMT and decommissioning phases of the plant. The submission sets out typical commissioning activities for each of the systems, as well as how at the detailed design stage, ‘Through Life Activity’ requirements will be established for maintenance activities associated with each of the systems.
3. I consider the RP’s recognition of the need to include through life management in the safety case and how it is important to ensure the design is developed considering its future delivery sufficient at this time, highlighting no fundamental concerns and is demonstrating an approach aligned to the ONR SAPs EMT.1 and EAD.1.
4. During GDA Step 3, as the detailed design develops, I will look to gain confidence that the RP can demonstrate processes are being established that ensure the design is developed with these SAPs in mind and can demonstrate that the principal electrical plant layout and architecture is such that the necessary EIMT or replacement activities can be undertaken whilst maintaining the required level of safety system availability.

### Support to human operations

1. It is my expectation that the electrical design is designed to support operators in fulfilling their safety roles, whether this be through the provision of appropriately robust lighting systems or communication systems to support local to plant actions or through station emergency alarm systems to protect personnel.
2. Whilst the RP has recognised the importance of such systems and included them within the scope for the GDA (ref. [13]), these systems or the underpinning analysis has not been developed at this time. I do not consider this a fundamental gap at this time but will expect the RP to be able to demonstrate that any human operations required to operate or maintain electrical equipment important to safety is considered during GDA Step 3.

### Smart Device strategy

1. Smart devices are instruments, sensors, actuators or other previously electro-mechanical components (e.g. relays, positioners and controllers) which are controlled by a built-in microprocessor or hardware description language programmable devices. They are becoming increasingly the only commercially available solution across both Control and Instrumentation (C&I) and electrical systems as manufacturers seek advances in functionality and self diagnostics whilst reducing development times and production cost. However, their complexity introduces new risks and makes it harder to demonstrate adequate reliability.
2. For GDA Step 2, I have considered if the RP recognises the risks from the use of such devices and if an appropriate strategy for their identification and use is being developed.
3. The Electrical Protection Philosophy and Smart Devices (ref. [31]) provides an overview of the RP strategy for the use of smart devices within the electrical system. The strategy sets out the high level benefits and risks from the use of smart devices and how there is an increasingly limited market for non-smart devices available.
4. Specifically considering protection relays, it is stated that it is the RP’s intention is to use smart devices for protection functions to detect faults which can’t be detected by non-smart devices or to support increased selectivity or disconnection speed. It is also stated that their use on Class 3 and Class 2 systems is likely, whilst on Class 1 systems is under review. I consider this a good strategy which will limit the need to undertake complex qualification.
5. (Ref. [31]) also identifies other electrical systems, including UPS and generator controls, where smart devices are likely to be proposed by future suppliers.
6. In the Electrical Design Rules (ref. [33]), the RP has identified specific requirements relating to the use of smart devices on electrical systems and the need to provide adequate analysis to demonstrate that the system capability is not jeopardised through the use of such devices. In addition, it identifies that smart devices should not be used in a system providing the power supply to the Class 1 DPS, which is consistent to the claim noted in paragraph ‎118, above.
7. I consider the recognition of the risks and benefits associated with the use of smart devices to be a positive consideration at this time. During GDA Step 3, as the design develops I will expect the RP to develop the strategy and requirements for their use to be further defined both in terms of the risk from individual device faults but also demonstrating the management of the risk of common cause failure from the potential use of components containing smart devices across multiple electrical systems, and meeting the expectations of ONR SAP EDR.3.
8. It is stated in (ref. [31]) that the RP’s approach to the use and qualification of smart devices, of all safety classes, is managed by the RP’s C&I team. I consider this a good practice which ensures a consistent strategy and qualification process is deployed across all components. I have worked with the ONR C&I Inspector, who is taking the lead on the assessment of this aspect (ref. [47]) during GDA for ONR
9. In summary, based on the outcome of my Step 2 assessment of the approach to the use of smart devices on the electrical system, I have concluded that the philosophy appears to be robust and consistent with ONR SAP EDR.3. Whilst the ONR C&I Inspector will continue to take the lead on the assessment of their approach to qualification, during GDA Step 3 I will continue to gain confidence that the RP is appropriately identifying where smart devices could and should be utilised in line with their risk strategy.

### Categorisation of safety functions and classification of systems, structures and components

1. I have assessed the RP’s approach to Categorisation and Classification (ref. [32]) in the context of electrical engineering. Since electrical systems do not generally provide safety functions directly, but instead deliver electrical power to SSCs that do, I consider that any RP process should reflect this.
2. I have considered ONR SAPs ECS.1 (Safety categorisation) and ECS.2 (Safety classification of structures, systems and components) as the basis for my assessment. The Categorisation and Classification TAG (ref. [18]) has been used to support my judgements together with IAEA Specific Safety Guide SSG-30 (ref. [20]) and BS IEC 61226 (ref. [25]).
3. The classification of the electrical distribution system is presented in the E3S Case Chapter 8 (ref. [5]), System Design Description (ref. [29]) and electrical single line diagrams (refs [44] and [43]), as well as in the Requirement Specifications for the respective systems (ref. [38]). At this time, these single line diagrams primarily highlight the more significant loads such as C&I systems and larger motors, such as RCPs or feedwater pumps. Whilst the electrical load schedule might shed more light on the allocation of lower powered safety systems, the current version (ref. [48]) only highlights the type of supply it is to be connected to (e.g. Essential or Main) without being specific on whether it needs to be resilient to LOOP, SBO or Total Loss of AC Power (TLACP) situations and does not identify the classification of the respective load.
4. I will expect during GDA Step 3 that as the RP develops a safety case that can articulate the flow from principles through analysis to requirements and design, the safety case ‘golden thread’, that the RP is able to show which precise switchboard each load is allocated to and why. However, from a review of how the C&I loads are allocated, I am content that the loads appear to be connected to switchboards at a level of defence which are supported by a power source, which is appropriately and consistently classified (i.e. a Class 2 or 3 C&I system is supported by a Class 2 switchboard and diesel generator; whilst the Class 1 C&I system is supported by Class 1 batteries).
5. Whilst the four division Class 1 DPS system is proposed to be supported by only two Class 3 Alternate AC Diesel Generators, the RP has indicated that this in line with (ref. [32]) and considers a time-based down-classification process. This has the potential to remove the expectation to provide multiple on-site standby generators that are required to be designed, manufactured and maintained to achieve the highest reliability expectations of Class 1. Whilst it is likely that the plant hazard, and therefore the categorisation of any safety function, will likely have reduced in the 24 hours before the batteries are discharged, it is not clear if a drop from Class 1 to Class 3 is substantiated. I will follow this up during Step 3 to ensure the RP is able to demonstrate this by analysis.
6. In summary, based on the outcome of my GDA Step 2 assessment of the approach to categorisation and classification of the electrical system, I have concluded that the fundamental approach and implementation appears to be robust and consistent with ONR SAPs ECS.1 and ECS.2 and BS IEC 61226 (ref. [25]). I will expect during Step 3 that any down-classification of SSCs is substantiated.

### Heating Ventilation and Air Conditioning of electrical equipment

1. In GDA Step 2, I have considered how the RP is considering the resilience of the design to low and high external ambient air temperatures and the operation of the electrical system based on information provided in E3S Case Chapter 8 (ref. [5]), System Design Description (ref. [29]) and engagements with the RP. This work has involved cross-discipline interactions with ONR inspectors from mechanical, internal and external hazards, and fault studies disciplines.
2. I have sought assurance that the RP was considering the need to ensure that spaces within the design that contain electrical equipment necessary to ensure a controlled and safe state of the plant will be kept within equipment temperature limits. I have also sought confidence that the RP is considering the need to provide adequate ventilation to any areas containing batteries, where the effects of charging may result in the build up of hydrogen gas.
3. In my assessment, I have considered the following SAPs (ref. [8]):

* EHA.14 (Fire, explosion, missiles, toxic gases etc – sources of harm).
* EKP.3 (Defence in depth).
* EKP.5 (Safety measures).
* EDR.2 (Redundancy, diversity and segregation).

1. I have considered the IAEA Specific Safety Guide SSG-62 (ref. [23]) as well as the ONR TAGs on Safety Systems (ref. [16]) and Essential Services (ref. [17]) to support my judgements.
2. I note that the RP is in the early stages of the design of the HVAC systems and that recent changes to the reactor island layout (ref. [49]) have impacted on the ability to demonstrate a robust and consistent architecture. In the various Requirements Specifications for the electrical systems (ref. [38]), the RP identifies that the electrical systems shall ‘interface with the HVAC systems in controlled areas and exclusion areas (KL)’ to ‘supply power to HVAC and receive heating/cooling and ventilation’. I consider these high level expectations show that the RP recognises the two-way dependency between HVAC and electrical; HVAC support may be required for the electrical systems as well as the need for electrical supplies for the HVAC system.
3. The specific Requirements Specifications for the DC systems (BQ and BP) (refs [40] and [39]), which define the various system batteries, also include expectations that they shall have hydrogen removed by the ‘KL’ HVAC system for safety reasons. I consider this important to reflect the potential for the build up of flammable gases without an adequate airflow.
4. In respect of functional categorisation and equipment classification, I note that the Requirements Specifications for the BQ system (ref. [39]), which defines the UPS systems which support Class 1 and Class 2 electrical systems, sets the HVAC related functions as Category A. The BP system requirements (ref. [40]), which define the requirements for the UPS systems which support Class 3 electrical systems, sets the HVAC related functions as Category C. Whilst these levels meet the expectations of the ONR SAPs in respect of categorisation and classification, the use of a single BQ system code for both Class 1 and Class 2 systems may result in the RP over-categorising the electrical supplies to the HVAC system that supports Class 2 SSCs. I will consider this as well as confidence that the RP is reflecting the different defence-in-depth role of the two BQ in design, maintaining independence between the corresponding HVAC systems, during GDA Step 3 as the RP develops the HVAC system design.
5. I have considered the basic architecture for the ‘KL’ HVAC system as presented in the System Design Definition (ref. [34]) and considered whether it meets the requirements set out above. (Ref. [34]) sets out how the electrical rooms are to be supported by the ‘KLE’ sub-system serving uncontrolled areas. This sets out how the KLE supply systems are to be largely unclassified, the ‘exception being local cooling units serving the Safety Classified C&I or electrical equipment, which are Class 1, 2 or 3 to match the classification of the C&I division being served’.
6. Whilst I consider this approach could meet the expectations set out in the Requirements Specifications for BP and BQ (Refs [40] and [39]) in respect of room cooling, I am concerned this may not set out what is required for the removal of hydrogen gas from rooms containing batteries.
7. I have engaged alongside other ONR disciplines during GDA Step 2 and the RP has indicated that the approach to HVAC system design is being reviewed following the recent layout changes (ref. [49]).
8. In summary, I consider that in principle the proposed HVAC approach could meet the expectations of the relevant ONR SAPs and the IAEA Safety Guide. I consider the design immaturity and recent layout changes are hindering the developing of a robust case. As part of GDA Step 3, I will look for the RP to demonstrate how the build-up of hydrogen within battery areas and control of local temperatures within electrical systems during all plant conditions will be managed.

### Use of Variable Frequency Drives

1. In the Electrical Power System Key Single Line Diagram (ref. [43]), I noted that the RP was intending to utilise variable frequency drives (VFD) to supply a number of pumps, including reactor coolant pumps and main feedwater pumps; some at high voltage.
2. Whilst the use of VFD when coupled to motor driven pumps or fans gives the flexibility to control pressure and flow rates or to reduce the power demand during pump startup, their use also presents additional risks, including reducing overall system reliability and introducing additional failure modes, all of which I expect to be considered in the overall safety consideration.
3. In my assessment, I have considered the following SAPs (ref. [8]):

* EDR.1 (Failure to Safety).
* ERL.1 (Form of claims).

1. Noting the limited information provided in the relevant E3S Case Chapters 5, 8 and 10 (refs [3], [5] and [6]), I have engaged with the RP during Step 2 and sought clarity through an RQ (ref. [35]) on where the intention is to utilise VFDs and gain confidence their use recognises and is appropriately considering the risks associated with their use, in defining the performance and operational requirements as well as impacts on the wider electrical systems.
2. The RP has set out the systems where it currently intends to utilise VFDs in the response to the RQ. With the limited information available at this time, I have focused my attention on the RP’s approach to those systems that I consider may have a greater nuclear safety impact, either directly or indirectly.
3. Whilst the RP only intends to utilise the VFDs supporting RCPs during reactor startup and since their operation do not support the delivery of SSCs that provide safety functions, the RP has identified the functional requirement as a non-categorised safety function. However, it does note that as part of the DR3 milestone, a review of the potential for direct and indirect consequences for all credible failure modes will be performed, which may affect this operational classification.
4. The types of failure modes the RP indicated in the RQ response that will be considered during a detailed failure modes and effects analysis did not appear to capture some potentially significant failure modes, such as uncontrolled overspeed or reverse direction. Both of these could have a significant impact on the functionality or integrity of the primary circuit.
5. However, follow-up engagement has indicated this failure mode will be considered as part of the RP’s Hazard and Operability Analysis (HAZOP) process required as part of the DR3 design decision point.
6. The RP has indicated that for the remaining motors that are to be controlled by VFDs, these operate across all modes of operation, and has indicated these are all considered to be Category C nuclear safety functions.
7. Through the identification of risks, initial categorisation and the need to undertake a HAZOP as part of design development, I consider the RP is taking steps to meet the expectations of ONR SAPs EDR.1 and ERL.1. From my engagement with the RP, whilst the detail is currently lacking, I consider this can be explained by the immaturity of the design rather than a fundamental shortfall. I will continue to engage with the RP during GDA Step 3 and will expect further clarity on the role of any VFDs together with safety categorisation and safety analysis that justifies their use and design.

### Grid Code compliance

1. The ability to connect the nuclear power plant to the GB transmission system through compliance with the The Grid Code (ref. [36]) is important not only from a commercial perspective but also from a safety perspective. Whilst ONR (ref. [50]) and IAEA (ref. [21]) expectations are that a facility should be able to provide power from on site sources to support delivery of the controlled and safe state, the normal, or preferred power supply, is from the offsite power supply, if available. In addition, it is important to ensure that technical compliance with the operational requirements of (ref. [36]), including the ability to provide frequency response, do not challenge nuclear safety.
2. In my assessment, I have considered whether the design is able to connect to the GB transmission system providing electrical supplies to equipment important to safety from and export power to the GB transmission system within the operational limits specified in (ref. [36]), without affecting nuclear safety.
3. In GDA Step 2, the RP has provided a strategy for assessing compliance with (ref. [36]). From a review of this, I consider that the RP has recognised the need to analyse and established a commitment to demonstrate compliance with the technical requirements of (ref. [36]) and is undertaking work on this analysis. I will consider the evidence that is produced from this analysis during GDA Step 3.

### ALARP

1. Without a detailed design, it is difficult to judge whether the design can be shown to have reduced risks so far is as reasonably practicable, or ALARP.
2. From the submissions assessed to date, I consider the RP is developing an electrical system that is consistent with the expectations of international good practice as set out in relevant IAEA technical guidance, as well as identifying and adopting national and international codes and standards for electrical equipment. This means that as the detailed design is completed, the RP should be able to demonstrate that the design is consistent with UK regulatory expectations.
3. As part of my GDA Step 2 assessment, I have assessed the decision record (ref. [51]), where the RP has down-selected technologies for standby generators and I consider the rationale is clear, well founded and specifically considers safety risk reduction as a high priority.
4. During GDA Step 3, as the design matures through the RP’s DR3 decision point, where the design requirements will be finalised and the design developed into a single solution, I will sample the evidence underpinning those decisions, including any HAZOP studies, to gain confidence that the processes used deliver a design that can be considered to reduce risks ALARP.

# Conclusions

## Conclusions

1. This report presents the GDA Step 2 Electrical Engineering 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 relevant E3S case chapters and supporting documentation provided by Rolls-Royce SMR Limited to form my judgements. I targeted my assessment, in accordance with my assessment plan, at the content of most relevance to electrical engineering against the expectations of ONR’s SAPs, TAGs and other guidance which ONR regards as relevant good practice.
2. Based upon my assessment, I have concluded the following:

* E3S Case Chapter 8 provides a good high level introduction to the role and purpose of the electrical system, in support of the safety functions. As the design matures, I will expect this to expand to explicitly identify any role it has in supporting safety, environmental and safeguards functions.
* Whilst the E3S Case Route Map provides an initial structure to the case and identifies the submissions considered at this step of the GDA assessment, I consider that as the RP identifies the evidence necessary to substantiate the role of the electrical system in the safety case, the RP may need to refine the breakdown of claims and arguments to ensure it is clear and comprehensive.
* The design is developing alongside the safety case, with a signficant design milestone, DR3, due progressively across systems within the year, which should provide the safety justification for the design.
* The design proposes a basic electrical distribution architecture that is consistent with IAEA guidance, providing a robust defence-in-depth capability.
* Design includes both Standby and Alternate AC Generators, together with provision of connection points for mobile generators, to provide supplies in a LOOP, SBO or TLACP event.
* It is not clear at this point that the mission times of the standby AC generators is consistent with the current expectations for a LOOP resulting from a nationwide event.
* The HVAC system design is immature and it is not currently clear how the RP intends to ensure the removal of hydrogen gas from battery areas during LOOP or SBO conditions.
* I have identified a number of areas where the safety case claims structure needs development and the evidence to underpin these claims needs to be identified. I consider these current shortfalls are linked to the immaturity of the design and the RP has indicated that as the design develops through the DR3 design point, the case will become more structured and evidential.

1. I shall consider each of these aspects further during GDA Step 3 and seek assurance that my concerns are appropriately addressed and justified in the safety case.
2. 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 nuclear power plant 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 3: E3S Objectives and Design Rules for SSCs, SMR0004589, Issue 3, May 2024. (Record ref. ONRW-2019369590-9885). |
| [3] | 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). |
| [4] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 7: Instrumentation and Control, SMR0003929, Issue 3, May 2024. (Record ref. ONRW-2019369590-9887). |
| [5] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 8: Electrical Power, SMR0004010, Issue 3, May 2024. (Record ref. ONRW-2019369590-9899). |
| [6] | 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). |
| [7] | 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. |
| [8] | ONR, Safety Assessment Principles for Nuclear Facilities (SAPs), 2014 Edition, Revision 1, January 2020. www.onr.org.uk/media/pobf24xm/saps2014.pdf. |
| [9] | ONR, Guidance on the Production of Reports for Permissioning and Assessment, NS-TAST-GD-108, Issue No. 1, December 2022. (CM9 ref. 2022/71935). |
| [10] | 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. |
| [11] | ONR, Step 2 Electrical Engineering Assessment Plan for the Generic Design Assessment of the Rolls-Royce SMR, ONR-GDA-AP-22-017, Issue 1, February 2023. (Record ref. ONRW-2126615823-394). |
| [12] | 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). |
| [13] | Rolls-Royce SMR Limited, Rolls-Royce SMR Generic Design Assessment Scope, SMR0002183, Issue 2, January 2023. (Record ref. ONRW-2019369590-7694). |
| [14] | WENRA, Safety Reference Levels for Existing Reactors 2020. February 2021. WENRA. www.wenra.eu. |
| [15] | 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. |
| [16] | ONR, Safety Systems, NS-TAST-GD-003, Issue 9.2, September 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-003.docx. |
| [17] | ONR, Essential Services, NS-TAST-GD-019, Issue 5.1, December 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-019.docx. |
| [18] | 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. |
| [19] | IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1, Rev. 1, February 2016. www.iaea.org. |
| [20] | IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide SSG-30, May 2014. www.iaea.org. |
| [21] | IAEA, Design of Electrical Power Systems for Nuclear Power Plants, Specific Safety Guide SSG-34, March 2016. www.iaea.org. |
| [22] | IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61, September 2021. www.iaea.org. |
| [23] | IAEA, Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants, Specific Safety Guide SSG-62, August 2020. www.iaea.org. |
| [24] | IAEA, Design Provisions for Withstanding Station Blackout at Nuclear Power Plants, IAEA-TECDOC-1770, August 2015. www.iaea.org. |
| [25] | BSI, Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems, BS EN IEC 61226:2021, July 2021. www.bsigroup.com. |
| [26] | BSI, Nuclear power plants - Electrical power plants - General requirements, BS EN IEC 63046:2021, June 2021. www.bsigroup.com. |
| [27] | Rolls-Royce SMR Limited, E3S Case Route Map, SMR0002155, Issue 3, November 2023. (Record ref. ONRW-2019369590-5998). |
| [28] | Rolls-Royce SMR Limited, Rolls-Royce SMR - GDA Design Reference Report, SMR0009043, Issue 2, April 2024 (Record Ref. ONRW-2019369590-8872). |
| [29] | Rolls-Royce SMR Limited, System Design Description for the Electrical Systems [A, B, MS, XF, XQ], SMR0006019, Issue 1, July 2023. (Record ref. ONRW-2019369590-3654). |
| [30] | Rolls-Royce SMR Limited, RR SMR EMIT Strategy (Examination, Maintenance, Inspection and Testing), SMR0009111, Issue 1, December 2023 (Record ref. ONRW-2019369590-5803). |
| [31] | Rolls-Royce SMR Limited, SMR Electrical Protection Philosophy and Smart Devices, SMR0005438, Issue 1, July 2023 (Record ref. ONRW-2019369590-3655). |
| [32] | 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). |
| [33] | Rolls-Royce SMR Limited, Electrical Design Rules, SMR0006010, Issue 1, September 2023. (Record ref. ONRW-2019369590-4433). |
| [34] | Rolls-Royce SMR Limited, System Design Description for the HVAC Systems Serving Controlled Areas and Uncontrolled Areas of Reactor Island (KL), SMR0004702, Issue 1, June 2023 (Record Ref. ONRW-2019369590-3723). |
| [35] | ONR, Schedule of Step 2 Regulatory Queries, April 2024. (Record ref. ONRW-2019369590-9071). |
| [36] | National Grid ESO Limited, The Grid Code, Issue 6 Revision 21, March 2024. www.nationalgrideso.com/industry-information/codes/grid-code-gc. |
| [37] | Rolls-Royce SMR Limited, National Grid (NG) Grid Code Compliance Strategy, SMR0005762, Issue 1, August 2023. (Record ref. ONRW-2019369590-4068). |
| [38] | Rolls-Royce SMR Limited, High Voltage AC Essential Supply Systems (BD) - Requirements Specification, SMR0004111, Issue 1, January 2023. (Record ref. ONRW-2019369590-3636). |
| [39] | Rolls-Royce SMR Limited, Low Voltage DC Electrical Supply System 1 for Safety Services [BQ] - Requirements Specification, SMR0004144, Issue 1, January 2023. (Record ref. ONRW-2019369590-3629). |
| [40] | Rolls-Royce SMR Limited, Low Voltage DC Electrical Main Supply System [BP] - Requirements Specification, SMR0004143, Issue 1, January 2023. (Record ref. ONRW-2019369590-3628). |
| [41] | ONR, Regulatory Observation - Development of the generic E3S case, RO-RRSMR-001, Revision 0, August 2023. www.onr.org.uk/media/k0odfpcf/ro-rrsmr-001.docx. |
| [42] | Rolls-Royce SMR Limited, BL System - Requirements Specification, SMR0004125, Issue 1, January 2023. (Record ref. ONRW-2019369590-3632). |
| [43] | Rolls-Royce SMR Limited, Electrical Power System Key - Single Line Diagram, SMR0001400, Issue 02, July 2023 (Record ref. ONRW-2019369590-3625). |
| [44] | Rolls-Royce SMR Limited, Essential Reactor Island - Single Line Diagram, SMR0006329, Issue 01, July 2023. (Record ref. ONRW-2019369590-3623). |
| [45] | National Grid Electricity System Operator Limited, GC0156: Facilitating the Implementation of the Electricity System Restoriation Standard, Final Modification Report GC0156, July 2023. www.nationalgrideso.com/document/284546/download. |
| [46] | ONR, Step 4 Assessment of Electrical Engineering for the UK HPR1000 Reactor, ONR-NR-AR-21-011, Revision 0, January 2022. www.onr.org.uk/media/documents/gda/uk-hpr1000/step-4/onr-nr-ar-21-011.pdf. |
| [47] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Control and Instrumentation, ONRW-2126615823-2965, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2965). |
| [48] | Rolls-Royce SMR Limited, Overall Electrical Load Schedule, SMR0000975, Issue 2, July 2023. (Record ref. ONRW-2019369590-3626). |
| [49] | Rolls-Royce SMR Limited, Reactor Island Architectural and Layout Summart Report, SMR0007298, Issue 1, January 2024 (Record ref. ONRW-2019369590-7011). |
| [50] | ONR, New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-GD-007, Revision 0, May 2019. www.onr.org.uk/media/c2delysl/onr-gda-007.pdf. |
| [51] | Rolls-Royce SMR Limited, D108 - Standby AC Generator Technology - Decision Record, SMR0003557, Issue 1, April 2023. (Record Ref. ONRW-2019369590-4813). |

# Appendix 1 – Relevant ONR SAPs considered during the assessment

|  |  |
| --- | --- |
| SAP No. | SAP Title |
| EKP.3 | Engineering principles: key principles – Defence in depth |
| EKP.5 | Engineering principles: key principles – Safety measures |
| ECS.1 | Engineering principles: safety classification and standards – Safety categorisation |
| ECS.2 | Engineering principles: safety classification and standards – Safety classification of structures, systems and components |
| EDR.1 | Engineering principles: design for reliability – Failure to safety |
| EDR.2 | Engineering principles: design for reliability – Redundancy, diversity and segregation |
| EDR.3 | Engineering principles: design for reliability - Common cause failure |
| EDR.4 | Engineering principles: design for reliability – Single failure criterion |
| ERL.1 | Engineering principles: reliability claims – Form of claims |
| EMT.1 | Engineering principles: maintenance, inspection and testing – Identification of requirements |
| EAD.1 | Engineering principles: ageing and degradation – Safe working life |
| EHA.14 | Engineering principles: external and internal hazards – Fire, explosion, missiles, toxic gases etc – sources of harm |
| ESS.8 | Engineering principles: safety systems – Automatic initiation |