|  |
| --- |
|  |
| ONR Assessment Report  Generic Design Assessment of the Rolls Royce SMR – Step 2 Assessment of Probabilistic Safety Analysis |



ONR Assessment Report

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

**Report Title**: Step 2 Assessment of Probabilistic Safety Analysis

**Authored by**: [Redacted]

**Report Issue No**: 1

**Document ID**: ONRW-2126615823-2692

**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 probabilistic safety analysis (PSA) 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 case.

I targeted my assessment, in accordance with my assessment plan, at the content of most relevance to Topic 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:

* Adequacy of the PSA technical requirements and PSA methodologies
* Adequacy of accident sequence modelling, fault tree modelling, human reliability modelling and data analysis in the Step 2 PSA
* Adequacy of the description of the PSA results and the associated limitations

The scope of the PSA at Step 2 is internal events at power only. There is no PSA for shutdown states, internal and external hazards, fuel route or fuel handling. There is also no level 2 or level 3 PSA.

The conclusions of my assessments are:

* In general the RP have produced methodology documents that apply standards and techniques that are recognised as relevent good practice (RGP) for PSA. However in many cases these methodologies have not yet been fully applied and therefore there are limitations and gaps in various aspects of the PSA.
* The RP has developed a set of PSA Technical Requirements in line with UK and international RGP. However, I have found shortfalls in the PSA Development Strategy. These shortfalls were linked to planning for adding the missing scope of the PSA, quality assurance and demonstrating how PSA is used to risk inform the safety case and design. I raised regulatory observation RO-RRSMR-002 and accepted a resolution plan from the RP. The RP have submitted initial documents to begin addressing the RO. I will follow up the closure of this RO in Step 3.
* Regarding fault tree modelling and the representation of passive systems, the RP has produced a methodology for Step 2 in line with UK and international RGP and have developed adequate modelling of some front line SSCs. I have identified shortfalls against UK RGP for a full scope PSA related to modelling of support systems and testing and maintenance which the RP intend to address in Step 3. Therefore I do not consider these shortfalls to be fundamental shortfalls for the Step 2 assessment. I will follow up these aspects in Step 3.
* Regarding the human reliability analysis (HRA), A single screening value has been assigned to all operator actions which skews the results of the PSA. There is a lack of task analysis, lack of maintenance modelling and simplistic quantification of human errors. This represents a shortfall against UK RGP for a full scope PSA. I do not consider these to be fundamental shortfalls for Step 2 as the RP have committed to improving these aspects and I will follow this up in Step 3.
* Regarding the hazards PSA, the RP have presented insufficient detail to form a judgement on the adequacy of the internal hazards assessment and I will seek further information in Step 3.
* Regarding the quantification of the PSA and results, due to the limited scope of the PSA at Step 2, no direct comparisons against ONR’s numerical targets seven, eight and nine can be made at this stage. I will seek further information in Step 3 to enable comparisons against the numerical targets.
* Regarding demonstration that risks are as low as reasonably practicable, the PSA documentation assessed so far has limited discussion on this topic. As part of closing out RO-RRSMR-002 the RP will have to demonstrate how the PSA has been used to inform the design and the safety case. I will follow up closure of the RO in Step 3.

Overall, based on my assessment to date of the limited scope PSA, 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 Reasonably Practicable

AOL Assessment of Limitations

ASF Alternative Shutdown Function

C&I Control and Instrumentation

CAE Claims Arguments Evidence

CCF Common Cause Failure

CDF Core Damage Frequency

CDHR Condenser Decay Heat Removal

DAC Design Acceptance Certificate

DHR Decay Heat Removal

DPS Diverse Protection System

E3S Environment, Safety, Security and Safeguards

ECC Emergency Core Cooling

ELOG Extended Loss of Grid

EUR European Utility Requirements

FMEA Failure Mode and Effects Analysis

GDA Generic Design Assessment

HBSC Human Based Safety Claim

HEART Human Error Assessment and Reduction Technique

HEP Human Error Probability

HMI Human Machine Interface

HPIS High Pressure Injection System

HRA Human Reliability Analysis

HVAC Heating Ventilation Air Conditioning

IAEA International Atomic Energy Agency

IEF Initiating Event Frequency

INL Idaho National Lab

LER Licensee Event Reports

LERF Large or Early Release Frequency

LOCA Loss of Coolant Accident

LUHS Local Ultimate Heat Sink

MCS Minimal Cutset

MSIV Main Steam Isolation Valve

NRC Nuclear Regulatory Commission

ONR Office for Nuclear Regulation

OPEX Operating Experience

PACE Probabilistic Accident Consequence Evaluation (software)

PCC Passive Containment Cooling

PDHR Passive Decay Heat Removal

PIE Postulated Initiating Event

PSA Probabilistic Safety Analysis

PSCS Passive Steam Condensing System

PWR Pressurised Water Reactor

RCP Reactor Coolant Pump

RD Reference Design

RDS-PP Reference Designation System for Power Plants

RGP Relevant Good Practice

RO Regulatory Observation

RP Requesting Party

RPS Reactor Protection System

RPV Reactor Pressure Vessel

RQ Regulatory Query

SAP Safety Assessment Principle(s)

SG Steam Generator

SMR Small Modular Reactor

SSCs Systems, Structures and Components

SSG Specific Safety Guide (IAEA)

TAG Technical Assessment Guide(s) (ONR)

THERP Technique for Human Error Rate Prediction

WENRA Western European Nuclear Regulators’ Association

Contents

[Executive Summary 3](#_Toc172700447)

[List of Abbreviations 5](#_Toc172700448)

[1. Introduction 8](#_Toc172700449)

[2. Assessment standards and interfaces 11](#_Toc172700450)

[3. Requesting party’s submission 14](#_Toc172700451)

[4. ONR assessment 22](#_Toc172700452)

[5. Conclusions 48](#_Toc172700453)

[References 51](#_Toc172700454)

[Appendix 1 – Relevant SAPs considered during the assessment 56](#_Toc172700455)

# Introduction

1. This report presents the outcomes of my probabilistic safety analysis (PSA) 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] and [5]) and supporting documentation.
2. Assessment was undertaken in accordance with the requirements of the ONR management system and follows ONR’s guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [6]). The ONR Safety Assessment Principles (SAPs) (ref. [7]), together with supporting Technical Assessment Guides (TAGs) (ref. [8]), have been used as the basis for this assessment.
3. This is a major report as defined in 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 PSA (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 that it intends to complete a three step GDA, with the objective of receiving a design acceptance certificate (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 (SSCs) 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 are therefore out of scope of this assessment:

* faults occurring during shutdown states
* faults occurring during fuel handling or fuel storage
* severe accidents and radiological consequences, including level 2 and level 3 PSA

1. My assessment has considered the following aspects:

* The RP’s postulated initiating event (PIE) and initiating event frequency (IEF) derivation to gain confidence in the methods for IEF derivation and accident mitigation claims including those claimed in addition to the deterministic lines of protection for the PSA.
* The associated documentation related to fault tree and event tree modelling, data analysis and human reliability analysis to enhance my understanding of the model and confirm the PSA provides an adequate representation of the design.
* The RP’s PSA results and PSA electronic model to understand the description of the level 1 PSA and the core damage frequency (CDF) associated with reactor internal initiating events during at power operating modes.
* The Assessment of Limitations Report to understand the potential risks associated with areas of the PSA which are not currently developed.

# 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. [7]) 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. [14]) 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. [15]), which represent good practices for existing nuclear power plants, and safety objectives for new reactors (ref. [16]).
4. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the TAGs (ref. [8]). The TAGs provide the principal means for assessing the PSA aspects in practice.

### Safety Assessment Principles (SAPs)

1. The key SAPs applied within my assessment are the PSA SAPs: FA.1, FA.10, FA.11, FA.12, FA.13 and FA.14. These are the fundamental SAPs relating to the development, validity, scope and use of PSA to support design of new facilities. The assessment section demonstrates how these SAPs have been used in my assessment.
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-005 – Regulating Duties to Reduce Risks to As Low as Reasonably Practicable (ALARP) (ref. [17])
* NS-TAST-GD-030 – Probabilistic Safety Analysis (ref. [18])
* NS-TAST-GD-063 – Human Reliability Analysis (ref. [19])
* NS-TAST-GD-096 – Guidance on Mechanics of Assessment (ref. [6])

### National and international standards and guidance

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

* IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61 (ref. [20])
* IAEA SSG-3 Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants (ref. [21])
* IAEA-TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) For Applications in Nuclear Power Plants (ref. [22])

## Integration with other assessment topics

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

* Interactions with fault studies related to their assessment of the fault schedule and the derivation of initiating events and their frequencies. The list of initiating events and their frequencies should have a common basis for both deterministic safety analysis and PSA.
* Interactions with fault studies on assessment of the transient analysis that underpins the success criteria in the PSA. My assessment is supported by fault studies views on the transient analysis as they are the lead specialism in this area. We worked together to understand the RPs safety case, fault schedule and the interactions between different systems.
* Interactions with internal and external hazards to form a consistent view of the PSA hazards methodology and the limitations described within it. My assessment of the PSA hazards methodology supports their assessments.
* Interaction with electrical engineering relating to the initiating event frequency for extended loss of offsite power faults and the mitigations presented by the RP.

## Use of technical support contractors

1. During Step 2 I have not engaged technical support contractors (TSCs) to support my assessment of the PSA aspects of the Rolls-Royce SMR.

# 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 PSA. It also identifies the documents submitted by the RP which have formed the basis of my PSA 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 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 PSA includes modelling of the key core cooling systems including condenser decay heat removal (CDHR), passive decay heat removal (PDHR) and emergency core cooling (ECC). The PSA also models the primary shutdown (scram) and secondary alternative shutdown function (ASF) systems. The PSA has simplistic control and instrumentation (C&I) and electrical modelling.
5. A high-level summary of each of the key safety measures follows.
6. The ECC provides the ‘first’[[1]](#footnote-2) protective safety function for large loss of coolant accidents (LOCAs) and intermediate unisolable LOCAs and the ‘second’[[2]](#footnote-3) protective safety function for all frequent faults (including intact circuit faults). It provides the principal means of delivering the heat removal safety function and is a class 1 safety measure, with three trains (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.
7. The safety measure acts in three phases. 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.
8. 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. PDHR does not protect against large LOCAs or unisolable intermediate LOCAs. 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.
9. Despite the name, PDHR comprises active systems in most of its documented variants. The key SSCs claimed as part of this safety measure are:
10. High pressure injection system (HPIS), which is a two-train (N + 1) pumped system required to maintain primary circuit inventory during small break LOCAs and mitigate primary circuit contraction as a result of cooldown.
11. 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).
12. 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, a greater number of control rods are required for shutdown and hold down, than in similar civil PWRs.
13. The ASF provides the second protective safety function for delivering control of reactivity and is a Class 2 safety measure. The ASF is an active safety measure, comprising the HPIS and the emergency boron injection system which controls reactivity via the injection of enriched potassium tetraborate solution into the core.
14. For Step 2 the RP’s PSA team has focussed on modelling the reactor island. The level of detail in the systems modelling reduces for systems further away from the reactor island. There is some simple consideration of the turbine island, while the cooling water island is modelled as a single super-component.

## 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 1.



Figure 1: 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. [20]), supplemented to include UK specific expectations and expanded to include the other E3S purposes.

## Summary of the requesting party’s E3S Case for PSA

1. The RP have written up their PSA in Chapter 15 of the E3S case (ref. [3]). The stated aim of the RP’s PSA is to demonstrate that nuclear safety risks to workers and the public are understood and acceptable and it is used appropriately throughout the plant lifecycle to manage these risks. This will be substantiated by showing that the PSA is:

* suitable and sufficient to support nuclear safety;
* used appropriately to support nuclear safety,
* demonstrates that radiological risks are acceptable and reduced to ALARP.

1. The full demonstration of this stated aim will only be possible once the design has progressed further into its lifecycle (it is currently at concept design stage) and once the PSA has incorporated all the information that will become available to reflect this maturing design.
2. Presently the scope of the PSA is limited and only outline risk insights can be gained to support this stated aim. A large programme of work is planned over several future versions of the PSA model to expand its scope and meet its stated aim. This will be documented in future iterations of the E3S Case.
3. Due to the evolving nature of the RR SMR design, the inputs to the PSA presented within issue two of the E3S case (ref. [3]) do not directly align to one design reference point (DRP) (ref. [23]). The safety measures and high-level success criteria are derived from the system design documents, produced as part of the reference design (RD) five baseline. These were based on version six of the fault schedule (ref. [24]) and the issue three version of the RR SMR definition of PIEs and IEFs document (ref. [25]) which were produced using inputs from RD5 with consideration of some subsequent modifications.
4. Component level information has been derived from system process & instrumentation diagrams (P&IDs) produced as part of the RD6 baseline. The electrical supply information has been derived from single line diagrams also produced as part of the RD6 baseline. The C&I initiation parameters are based on the C&I engineering schedule which was additionally produced as part of the RD6 baseline. The first DRP corresponds to RD7 so none of the inputs to the PSA at Step 2 are aligned to the DRP. This information is summarised in Table 1.

**Table 1: Input Information for the Step 2 PSA**

|  | RD5 | RD6 |
| --- | --- | --- |
| Safety measures and high-level success criteria | X |  |
| Definition of PIEs and IEFs | X |  |
| Component level information for system models |  | X |
| Electrical supply information |  | X |
| C&I initiation parameters |  | X |

1. The RP has set out a series of claims on the PSA based on the E3S case route map (ref. [26]). The overarching claim is:

* The probabilistic safety assessment demonstrates that nuclear safety risks to workers and the public are understood and acceptable and is used appropriately throughout the plant lifecycle.

1. The project has set out a series of risk targets. These are captured in table 3 of the PSA technical requirements (ref. [27]). In addition to targets aligned to numerical targets five to nine from ONRs SAPs (ref. [7]) there are also targets of 1 × 10-05/1 × 10-07/yr[[3]](#footnote-4) for CDF and 1 × 10-06/1 × 10-08/yr for large or early release (LERF). While ONR does not set targets for CDF/LERF this is common in Europe and the United States.
2. The aspects covered by the Rolls-Royce SMR safety case in the area of PSA can be broadly grouped under four headings which are summarised as follows:

**The probabilistic safety assessment is suitable and sufficient to support nuclear safety**

1. The RP have made a claim that by the end of GDA the PSA will:

* consider all initiating events with potential to cause radiological exposure to people on-site or off-site
* consider all significant sources of radiation on the site
* consider all permitted operating states of the site
* use best estimate approaches wherever practicable
* provide an adequate representation of the design, its behaviour, and its operation.

**PSA is used appropriately to support nuclear safety throughout the plant lifecycle**

1. The RP have made a claim that by the end of GDA the PSA will:

* be used, where appropriate, to inform the design and operation of the site and its facilities, and emergency planning
* be used, where appropriate, to inform the provision of measures to mitigate the potential for significant radiological consequences.
* be used, where appropriate, to inform qualification requirements.

**The PSA demonstrates that radiological risks are acceptable**

1. The RP have indicated they will provide indicative numbers to substantiate as far as possible during GDA:

* quantify the frequency of significant fuel damage and the frequency of large or early release, assess them against project risk targets, and demonstrate that they have been reduced ALARP
* quantify the frequency of death of a person on the site from accidents at the site resulting in exposure to ionising radiation, assess it against project risk targets, and demonstrate that it has been reduced ALARP
* quantify the frequency of any single accident giving an effective dose to any person on-site, assess it against project risk targets, and demonstrate that it has been reduced ALARP
* quantify the frequency of death of a person off the site from accidents at the site resulting in exposure to ionising radiation, assess it against project risk targets, and demonstrate that it has been reduced ALARP
* quantify the frequency of accidents giving an effective dose to any person off-site, assess it against project risk targets, and demonstrate that it has been reduced ALARP
* quantify the frequency of 100 or more fatalities from accidents at the site resulting in exposure to ionising radiation, assess it against project risk targets, and demonstrate that it has been reduced ALARP

1. The current scope of the PSA is insufficient to allow the RP to demonstrate that all these claims have been met. The current PSA has been developed to evaluate risks inherent in the RP’s design for internal events at power with all relevant systems in their normal duty line up prior to the occurrence of a fault.

**ALARP**

1. The demonstration of ALARP is intended to be addressed by the comparison of the PSA results against the various numerical targets outlined in the section above. Each target should have an accompanying discussion as to whether there are any further risk reduction measures available that could be implemented.
2. The RP have produced an ALARP Summary Report (ref. [28]) which provides a summary of how the Rolls-Royce Small Modular Reactor reduces risks to ALARP at RD7 achieved in November 2023. This is the main reference supporting the E3S case Chapter 24 on ALARP (ref. [5]).

## Basis of assessment: requesting rarty’s documentation

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

* Rolls-Royce SMR Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies revision 2 (ref. [29]) and revision 4 (ref. [30]) which identifies the PIEs that will be modelled in the PSA and assigns initiating event frequencies.
* The PSA Technical Requirements (ref. [27]) and PSA Development Strategy (ref. [31]) which outline the overall approach to development of the PSA throughout the course of GDA.
* PSA Event Sequence Modelling Methodology (ref. [32]) and PSA Event Sequence Modelling Report (ref. [33]) which outline the approach to event sequence and event tree development and documents the accident sequences present in the Step 2 PSA.
* PSA SSC Modelling Methodology (ref. [34]) and PSA SSC Modelling Report (ref. [35]) which outline the approach to fault tree development and report the development of the fault trees present in the Step 2 PSA.
* Human Based Safety Claim (HBSC) Modelling Methodology (ref. [36]) and PSA Operator Action Modelling Report (ref. [37]) which outline the approach to operator action identification and document the human reliability modelling present in the Step 2 PSA.
* Data Methodology (ref. [38]) and PSA Data Notebook (ref. [39]) which present the methodology and reliability data selection for SSCs.
* PSA Hazard Event Modelling Methodology (ref. [40]) which outlines the methodology for hazard progression modelling.
* PSA Main Report (ref. [41]) which presents the overall PSA for the project. It provides an overview of the PSA model, the modelling performed to produce it and the results derived from it.
* PSA Assessment Of Limitations (ref. [42]) which presents the limitations of the Step 2 PSA and the potential impact of the resolution of limitations against the numerical risk targets.
* ALARP Summary Report (ref. [28]) which provides an overview of the decision-making processes that have been used up to RD7 and how PSA has informed decisions.

1. Consistent with ONR’s ‘guidance to requesting parties’ (ref. [10]), where I have identified gaps in the RP’s submissions, I have raised regulatory queries (RQs) (ref. [43]). More significant shortfalls against regulatory expectations are captured by issuing regulatory observations (ROs). At the time of writing I have raised 6 RQs and 1 RO to facilitate my assessment. These are discussed in the detailed assessment that follows.

# ONR assessment

## Assessment strategy

1. I considered all the main submissions within the remit of my assessment scope, to various degrees of breadth and depth. I chose to concentrate my assessment on those aspects that I judged to have the greatest safety significance, or where the radiological risks appeared least well controlled. My assessment was also influenced by the claims made by the RP and my previous experience of similar systems for reactors and other nuclear facilities. A particular focus of my assessment has been the RQs and RO I raised as a result of my on-going assessment, and the resolution thereof. I found that the tier 1 chapters and tier 2 and 3 submissions were consistent with each other
2. In line with ONR’s guidance and my assessment plan the main areas targeted were:

* review of supporting documents from other disciplines providing inputs to the PSA such as fault studies PIE and IEF documents
* review of the scope of the PSA
* review of the quality and adequacy of level 1 PSA event tree methodologies and modelling, including success criteria
* review of the quality and adequacy of level 1 PSA fault tree methodologies and modelling, including the treatment of passive systems and the representation of the design
* review of the RP’s data analysis
* review of the RP’s human reliability analysis
* review of the risk significant sequences in the PSA electronic model which forms the basis for the PSA, including the results for level 1 internal events
* review of the hazards analysis methodology
* review of the limitations of the PSA at the end of Step 2
* review of evidence that demonstrates there is a process in place to capture, track and review PSA assumptions to enable these assumptions to be captured in future stages of NPP development.
* review of evidence that demonstrates that there is a process of communication between Rolls Royce SMR Limited’s different technical departments and their PSA team

## Assessment

### Assessment of initiating event identification and initiating event frequencies

1. ONR’s SAP FA.13 outlines the expectation that best-estimate methods and data should be used as far as possible within the PSA and in particular for determining initiating event frequencies and in the supporting transient, accident progression, source term and radiological analyses. More detailed expectations for derivation of initiating events are outlined in Table A1-2.1 of NS-TAST-GD-030 (ref. [18]) and IAEA TECDOC-1804 (ref. [22]). IEFs should be derived on a best-estimate basis for use by both the deterministic safety analysis and PSA to present a common starting point for the safety analysis.
2. I assessed the Definition of Postulated Initiating Events And Derivation of Initiating Event Frequencies Report (ref. [29]) against IAEA standards and ONR guidance. The assessment of the supporting Hazard Log Report and Fault Schedule was carried out by my fault studies colleagues (ref. [44]).
3. The RP has identified the list of initiating events (IEs) through systematic analytical methods such as hazard and operability (HAZOP) analysis and failure mode and effect analysis (FMEA) on the RD6 and RD7 design. The RP has based their IEF values on operating experience (OPEX) in the form of licensee event reports (LERs) from the USA according to Nuclear Regulatory Commission (NRC) regulations. This data is high quality because Idaho National Lab (INL) take care to only include unplanned reactor transient events and carry out statistical analysis of different initiating events to ensure that the baseline period reflects a time period where the frequency of a given IEF has been constant. The RP has not justified the use of US data for a UK project which I will follow up in Step 3.
4. I initially assessed revision two of the Definition of PIEs and Derivation of IEFs document (ref. [29]). This document was using the original version of NUREG 5750 (ref. [45]) as the source of IEF data. Because NUREG 5750 is thirty years old this led to a small number of IEFs being overestimated due to the reduction in most IEFs over the past thirty years. This issue was addressed in revision four of the Definition of PIEs and Derivation of IEFs Report (ref. [30]) which moved to using the 2020 update of NUREG 5750 (ref. [46]) which captures data from the US fleet from 1988-2020. However, the PSA for Step 2 is based on the IEFs from revision two of the Definition of PIEs and Derivation of IEFs document so this leads to some conservatism in the PSA results. I do not consider this a significant issue because the change in IEFs is small and the RP will align the PSA with the latest version of the IEFs in 2024.
5. The RP have used the INL data where they have been able to match it to their list of PIEs. Where the INL data does not show any failures for a particular initiating event the RP have considered using a ‘half-tomorrow’ approach where they assume a single failure occurs in double the time captured by operating experience. This is likely to lead to conservative IEFs as the RP generally compared against the ‘PWR general transient’ fault group which only included 300 reactor critical years covering 2016-2020. However, in many cases the RP have not used the half-tomorrow IEF as they consider it to be overly conservative. I do not consider this a significant issue because this approach has been used by other licensees and previous RPs, and this level of conservatism is likely to be small compared to other sources of uncertainty in the PSA such as missing scope and transient analysis.
6. The RP has developed loss of grid IEFs based on ONR guidance provided as part of the Advanced Boiling Water Reactor GDA in 2017 (ref. [47]). Since this time ONR’s understanding of the likelihood of extended loss of grid (ELOG) faults has improved, such that ELOG faults are considered to be more likely than the RP’s documentation suggests. This concern was raised to the RP in a letter (ref. [48]) which explained the situation and suggested alternative IEFs for these faults. The RP have indicated they will hold discussions with National Grid during Step 3 but have not yet updated the frequency of the ELOG fault. The lack of consideration of this fault is a shortfall against ONR expectations and given the high risk significance of the ELOG fault in the PSA, equivalent to 33% of CDF, (see Section 4.2.8) this will be a focus of my assessment in Step 3.
7. The list of PIEs modelled in the PSA are aligned with the deterministic fault schedule. Non-deterministically derived faults such as those falling below the design basis cut-off frequency are not currently modelled. There may be impacts on the level 2 PSA if faults impact the reactor and containment or reactor and spent fuel pool simultaneously. This limitation has been recognised by the RP and they intend to address it during Step 3. I will follow up this aspect in Step 3.
8. There are various PIEs included in the definition of PIEs and derivation of IEFs document which are not yet included in the PSA, for example shutdown faults and fuel handling faults. I have not assessed these PIEs and IEFs at this time but expect to during Step 3 when they are incorporated into the PSA.
9. The Definition of PIEs and Derivation of IEFs document includes spurious C&I failure faults. The IEF for faults associated with class 2 systems is set at 1 x 10-2/yr which is a typical though likely conservative approach. It is positive to note that the RP has identified spurious C&I faults at an early stage in the project. However, the design of the C&I systems is not complete and therefore the list of spurious IEs is also not complete. I will follow up this aspect in Step 3.
10. The RP have compared their list of IEs against the European Utility Requirements (EUR), AP1000, IAEA and NUREG lists of IEs. For each of these IEs the RP has noted that they need to be added in a future revision or presented a justification for why they are not included. This process provides confidence the RP have captured most applicable IEs for their design which represents a positive aspect of the identification of IEs.
11. There are various other aspects of the design which have limited design maturity and therefore limited PIE identification. These include faults related to heating ventilation air conditioning (HVAC) systems, spurious actuation of C&I systems, fuel route operations and shutdown faults. Therefore at this stage the RP have not identified all faults having the potential to lead to any person receiving a significant dose, but they have established a process which I have confidence will adequately identify PIEs and derive IEFs for the design.
12. 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 relevant good practice (RGP) and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.

### PSA scope and PSA development strategy

1. ONR expectations for the scope and extent of PSA are outlined in SAP FA.12 which states that the PSA should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults. More detailed expectations for PSA scope are outlined in Table A1-1.2 of NS-TAST-GD-030 (ref. [18]).
2. The RP submitted their PSA Technical Requirements (ref. [27]) which outline the requirements the RP have placed on the PSA. The Technical Requirements call for a full scope, best-estimate PSA covering all relevant faults and hazards in all operating modes. I assessed the Technical Requirements and confirmed that they were in line with national and international RGP as set out in ONR (ref. [18]) and IAEA (ref. [21]) guidance.
3. At Step 2 the RP have provided a level 1 PSA that considers initiating events for at power modes 1 and 2, for reactor-based faults. There are no faults for shutdown modes (3-6), and the fuel route and spent fuel pool are not considered. There is no hazards modelling for internal or external hazards. There is no level 2 or level 3 PSA modelling. This means that a significant programme of updates is required for the RP to meet their stated aim of a full scope PSA. This scope does not meet ONR expectations for a full scope PSA during GDA.
4. The RP submitted Issue 1 of their PSA Development Strategy (ref. [49]) to demonstrate how the PSA would be developed throughout the duration of GDA. The RP indicated their intention to develop, within GDA timescales, a full-scope modern-standards PSA.
5. I assessed the PSA Development Strategy and found a number of shortfalls in the strategy:

* the RP did not explain how PSA would be integrated into the safety case
* the RP did not explain how PSA would be integrated into the design or how the PSA team should interact with other departments within the RP
* the RP did not explain the scope of the PSA
* the RP did not describe how the radiological risks to on-site workers will be evaluated
* the RP did not explain which radioactive sources would be considered by the PSA
* the RP had limited human resources and did not explain how the significant gaps in the scope would be delivered
* the RP did not explain the development plans for the hazards and severe accidents aspects of the PSA.
* the RP did not have PSA-specific quality assurance procedures in place

1. Based on my assessment I raised Regulatory Observation RO-RRSMR-002 (ref. [50]) to ensure that the RP addressed these gaps during GDA. The RO placed four actions on the RP:

* action 1 - provide a PSA project plan to cover GDA and address the limitations outlined in my assessment
* action 2 - submit to ONR the relevant PSA QA plans and procedures that detail the necessary level of quality assurance for each PSA task
* action 3 - demonstrate how the PSA is integrated into the wider safety case and will be used to support demonstration that risks have been reduced ALARP
* action 4 - demonstrate how the PSA is integrated into the development of the generic design

1. The RP responded to the RO by writing a resolution plan (ref. [51]) which was accepted by ONR. The resolution plan commits to the following updates:

* update of the PSA Development Strategy and production of a Step 3 Scope and Deliverables Document to address Action 1
* creation of a Performance and Use of PSA standard to set out the framework within which PSA is conducted to address Actions 1 to 4
* update of the PSA Hazard Event Modelling Methodology to provide further details on the plans for hazards PSA to address Action 1
* creation of a PSA Quality Plan to provide details of quality assurance arrangements to address Action 2
* demonstration of PSA integration into the safety case via the PSA Main Report (ref. [41]), ALARP Summary report (ref. [28]) and E3S Case Chapter 15 (ref. [3]) to address Action 3
* demonstration of PSA informing the design to address Action 4

1. The update to the PSA Development Strategy has been submitted. I have reviewed the updated PSA Development Strategy (ref. [31]) against the resolution plan.
2. The RP have clarified

* the scope of the PSA and the work expected to be produced during Step 3
* that they will consider fuel in the reactor and fuel route during GDA, with other radioactive sources considered post-GDA.
* their intention to eventually use the PSA as a risk monitor and to risk inform operations.
* their intention to use the PSA to support worker risk assessments, noting that additional methods still need to be produced.
* their hazards PSA methodology, but more information is required to understand what will be produced during GDA which should be submitted early in Step 3

1. Overall I consider that the RP has provided confidence that an adequate PSA can be produced during GDA. I will assess the closure of the RO once all the submissions have been made which is scheduled to be during 2024.
2. In summary, while the PSA Technical Requirements are adequate, because of the shortfalls that I have identified against UK RGP as noted above I have raised RO-RRSMR-002. I will follow up the closure of this RO during Step 3.

### Event tree methodologies and modelling

1. ONR expectations for event tree modelling are laid out in SAP FA.13 which states that the PSA model should provide an adequate representation of the facility and/or site. Table A1-2.3 of NS-TAST-GD-030 on PSA (ref. [18]) and Section 5 of IAEA SSG-3 (ref. [21]) provide further guidance on event tree modelling.
2. The RP has produced methodology documents for event sequence modelling (ref. [32]) and a report documenting the event sequence modelling (ref. [33]). I assessed these reports, and the accompanying PSA model, to compare the RPs approach to event tree modelling against RGP.
3. The Event Sequence Modelling Methodology (ref. [33]) sets out the approach that is intended to be followed for event sequence development. In line with the PSA Technical Requirements (ref. [52]) the methodology requires the PSA to be developed in a best-estimate and symmetric manner. The methodology only covers internal events at power in line with the scope of the PSA at Step 2. I consider that the methodology is in line with national and international RGP as set out in ONR (ref. [18]) and IAEA (ref. [21]) guidance.
4. I assessed the Event Sequence Modelling Report (ref. [34]) and a selection of event trees linked to the most risk significant faults in the PSA model to review how well the RP has implemented their methodology during Step 2.
5. ONR’s expectation is that best-estimate transient analysis is used to support the PSA. The document does not describe the transient analysis that supports the PSA. I queried this via RQ with the RP who noted that transient analysis work is still ongoing for many faults. At this stage of the project no best-estimate transient analysis has been undertaken by the RP. This is because the design is still at an early stage of maturity and the transient analysis carried out so far (ref. [53]) has been used to support the deterministic safety case and sizing studies for SSCs.
6. At this point in the project the RP have modelled the success criteria of systems based on their design intent, for example one out of three trains of ECC are required for faults. This may lead to optimistic modelling being developed if the SSCs are later found to not meet their design intent for all faults. This is an aspect the RP should improve as more detailed transient analysis becomes available. I will follow this up in Step 3.
7. The RP have modelled the event sequences in line with the deterministic fault schedule and have made additional claims on other mitigating systems where possible. It is positive that the RP have aligned the PSA with the fault schedule as this was not the case at the start of Step 2, but it is likely that as further analysis is carried out more mitigating claims will be identified. During Step 2 the PSA has been aligned with revision six of the fault schedule (ref. [24]) which covers reactor modes 1 and 2. This will be updated during Step 3 to cover all modes of operation.
8. The consequences assigned to fault sequences in the PSA are key to identifying whether the numerical targets are met. No radiological consequence analysis has been submitted at this time. To mitigate this limitation the RP currently have a simplistic approach to modelling the consequences of accident sequences. This approach is captured by two key assumptions in the Event Sequence Modelling Report. For each accident sequence the consequence is either noted as

* RFSS - no fuel degradation or damage, or
* RFMF - total melt of all fuel assemblies

1. This approach is acceptable for a purely level 1 PSA modelling core damage, but further information will need to be developed by the RP to enable development of a level 2 PSA during Step 3.
2. At this time no detailed modelling of plant damage states has been submitted but this will be addressed during Step 3 with the development of the level 2 PSA. Documents to define severe accident phenomena and radiological release categories will also be developed in Step 3.
3. The RP have set out a series of radiological targets which align with the ONR SAPs numerical targets. Due to the lack of radiological consequences modelling in Step 2 it is not possible to make meaningful comparisons against the numerical targets. The RP are intending to develop radiological consequences using the Probabilistic Accident Consequence Evaluation (PACE) tool produced by the UK Health Security Agency. The radiological consequences inspector will take the lead on assessing this.
4. To conclude, the development and use of event tree modelling is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence. However, insufficient detail has been presented to form a judgement on the adequacy of best-estimate transient analysis, plant damage modelling and radiological consequences and I will seek further information in Step 3.

### Fault tree methodologies and modelling

1. ONR expectations for fault tree modelling are laid out in SAP FA.13 which notes that the PSA should be detailed enough to capture dependencies and model all relevant failure modes of SSCs. Further guidance in available in Table A1-2.4 of NS-TAST-GD-030 on PSA (ref. [18]) and Section 5 of IAEA SSG-3 (ref. [21]). The RP has produced a methodology document for SSC modelling (ref. [34]) and a report documenting the SSC modelling (ref. [35]) in the Step 2 PSA. I assessed these reports, and the accompanying Step 2 PSA model, to compare the RPs approach to fault tree modelling against RGP.
2. The SSC Modelling Methodology (ref. [34]) sets out the approach for modelling fault trees in the PSA and the identification system used to link components in the design with those in the PSA. It also sets out the approach to modelling of common cause failures, success criteria and C&I systems. The methodology only covers internal events at power in line with the scope of the PSA at Step 2. I assessed the methodology to establish if it aligns with RGP.
3. The RP have set out an approach to fault tree modelling for internal events at power that meets RGP. The fault trees are set up to be able to run standalone to allow reliability modelling of individual systems which can help inform the designers where reliability of systems could be improved. The RP have proposed a small event tree / large fault tree approach. This means that human actions and support systems are included in the fault trees rather than having separate entries in the event trees. I have no concerns with this approach.
4. The RP have aligned the naming system in the PSA with the Reference Designation System for Power Plants (RDS-PP) identification system used across the project. This is a positive development which will enable easier use of the PSA to inform the design and allow other disciplines to more easily understand the PSA results.
5. To model common cause failure (CCF) the RP have used the alpha factor model and utilised the CCF modelling tools incorporated into the RiskSpectrum software. This meets RGP for CCF modelling and is a positive feature of the PSA model. The CCF tool in RiskSpectrum has limitations related to large CCF groups. Where a group size is larger than eight components the PSA tends to default to using the ‘All’ failure mode which fails all equivalent components in the model. This is a known limitation and should not affect the results significantly. The data the RP have used to quantify the CCFs is discussed in the following section on data analysis. Overall I consider that the SSC Modelling Methodology meets RGP and forms a sound basis for future fault tree modelling.
6. I assessed the SSC Modelling Report to review how well the RP has implemented it during Step 2. I raised RQ-01203 (ref. [43]) on the PSA SSC Modelling Report.
7. The RP have focussed their effort on modelling the reactor island along with simplified modelling of the turbine island. The cooling water island is only represented a single supercomponent. This is acceptable for Step 2 as the design is less susceptible to cooling water faults than typical PWRs as the plant has indirect cooling towers which do not need a continuous supply of seawater. The RP confirmed in their response to my RQ that they would improve the modelling of the turbine island and cooling water island in Step 3 to ensure that any dependencies between systems are captured.
8. The Step 2 PSA fault trees do not directly correspond to a particular design reference, being based on documents from both RD5 and RD6. This is typical for PSA as often input information is not all aligned to a particular point and PSA has its own development time which needs to be accounted for in planning. Whilst this is acceptable for Step 2, during Step 3 the RP will need to align the PSA model to a DRP or produce a gap analysis between the PSA and the DRP.
9. There is currently no consideration of testing or maintenance in the PSA model. This is a significant and optimistic limitation of the PSA which is being tracked as an assumption by the RP. I queried this limitation in RQ‑01203 (ref. [43]). The RP responded that this limitation will be addressed during Step 3 when testing and maintenance information becomes available. Because the current PSA model is for internal events at power, and I expect limited testing or maintenance to be carried out on reactor systems at power (based on typical practice for PWRs) I consider that this limitation does not undermine the insights of the Step 2 PSA. However, I will be following this up in Step 3 to confirm improvements are made in this area.
10. Support systems include HVAC, electrical supplies and C&I systems. I reviewed the support systems modelling in the PSA.

* There is no consideration of HVAC systems in the PSA model or associated documents. The RP have stated that their design intent is that HVAC systems will not be highly classified, however previous assessments for other reactor designs have shown that HVAC failures can lead to numerous other failures so this is an aspect that requires improvement which I will follow up in Step 3.
* The electrical supplies system modelling is also limited. The electrical distribution system for the reactor island is modelled. Whilst power supplies to pumps are modelled there are no power supplies modelled to the valves on the plant. I queried this limitation in RQ-01203 (ref. [43]) and the RP indicated that this would be addressed during 2024. Other aspects such as load shedding and reloading onto diesel generators following a loss of offsite power are also not modelled. The design is less susceptible to diesel generator failures than other PWR designs due to AC power not being required for any class 1 systems. The current level of detail in the electrical modelling is broadly aligned with the rest of the PSA model but this is an aspect of the PSA that requires improvement which I will follow up in Step 3.
* The C&I systems are modelled in a simplistic manner. There is no modelling of the processing or voting parts of the C&I systems. Single platform-level CCF events are being used to model the reactor protection system (RPS) and diverse protection system (DPS) systems with no consideration of operating system, application system or communication system aspects. On a positive note the sensors linked to the C&I systems are modelled explicitly along with their electrical supplies. The current level of detail in the C&I modelling is broadly aligned with the rest of the PSA model but I will follow up in Step 3 to confirm that improvements are made.

1. All three of these aspects are significant and likely optimistic limitations of the PSA at Step 2. While the CDF will definitely be impacted when the modelling is improved, I consider that the existing electrical and C&I modelling is sufficient to identify any fundamental shortfalls in the systems modelled so far. At this stage of the project these limitations do not undermine the insights of the Step 2 PSA, but I will be following this up in Step 3 to confirm improvements in this area.

#### Passive systems modelling in PSA

1. The Rolls-Royce SMR design incorporates a number of passive (or partially passive) systems. This is encouraged by ONR, for example SAP 155 notes that safety should be secured by passive safety measures that do not rely on control systems, active safety systems or human intervention. The notable passive systems in the RP’s design are the ECCS (which includes the PCC heat exchangers) and the PDHR system.

#### ECCS

1. The ECCS is a class 1 system claimed as the only safety function for heat removal for infrequent faults and the second protective safety function for heat removal for most frequent faults. The ECCS is comprised of three trains and one train is required for success in all faults where it is claimed. The ECCS is comprised of three phases:

* Phase 1 – High pressure (HP) blowdown and accumulator injection
* Phase 2 – Low pressure (LP) blowdown and gravity drain
* Phase 3 – Recirculation and decay heat removal (DHR) via PCC heat exchangers and LUHS

1. All three phases require signals for initiation, while accumulator injection, gravity drain, and recirculation are passive.
2. The RP have modelled the significant components of the ECCS in the PSA. The ECCS includes a pair of valves to control blowdown while minimising the risk of spurious ECC initiation which represents a LOCA due to the breach created in the primary circuit. The high-pressure emergency blowdown valve is somewhat novel. It is a combination of valves that will only allow blowdown when the primary circuit pressure is >16bar or <10.5 bar. The PSA has modelled this valve as a normal relief valve. A multi-stage control valve is also in series with the emergency blowdown valve. This valve has been modelled as a typical motor operated valve which may not reflect the complexity in the control of this valve which allows for a controlled depressurisation of the primary circuit. At this stage of development of the PSA this modelling is adequate due to a lack of design specific data, but this should be improved in the future when reliability data for the valves are available.
3. Fault Tree analysis of the ECCS shows that the most significant failure modes are:

* CCF of the PCC heat exchangers due to tube blockages
* CCF of the filters in the refuelling pool due to filter blockage
* CCF of the filters in the containment sump due to filter blockage
* CCF of the high-pressure blowdown pilot relief valves
* CCF of the low-pressure blowdown pilot relief valves
* CCF of the multistage automatic isolation valves

1. The passive circulation parts of the system are not explicitly modelled in the PSA, apart from the heat exchanger tube blockages. This effectively means the RP are assuming ECC is completely reliable once the system has been initialised. Substantiation of this will be required, primarily supported by RELAP, VIPRE, CASMO5, SIMULATE5 and GOTHIC modelling. The fault studies topic is leading on the assessment of these aspects. The RP may need to include further failure modes based on HAZID information for the ECCS, plus an additional failure mode to represent the uncertainty that the system will passively function. I will follow this up in Step 3.
2. For the PCCS which supports ECC there are eighteen separate heat exchangers modelled in the PSA in three groups of six. Failure of one heat exchanger in each group of three will lead to the overall PCCS failing in the PSA, whereas only six of the eighteen heat exchangers are required for success if they are from the same group. Because the PSA software cannot adequately model CCF groups this large the risk is dominated by the all-modes failure CCF. More detailed transient analysis would likely indicate that this approach is conservative. I will follow up the modelling of the ECCS in Step 3 to confirm if best-estimate modelling can be developed by the RP.

#### PDHR

1. The PDHR system is a class 2 system claimed as the first protective safety function for most frequent faults. The PDHR has three cooling loops which have success criteria of one out of three, along with two HPIS trains which have success criteria of one out of two. The PDHR requires a number of active components to work for the passive cooling loop to be established. No operator actions are required to initiate the system, but an RPS signal is required (based on low SG level) to trigger the initialisation of the system. This leads to:

* isolation of main steam isolation valves (MSIVs)
* isolation of the hot legs of the SGs
* isolation of the SG blowdown containment valves
* blowdown of the secondary circuit via the atmospheric steam dump (ASD) system

1. Additionally The HPIS is assumed to be required to maintain primary circuit inventory during small break LOCAs and mitigate primary circuit contraction because of cooldown during intact circuit faults. Some preliminary analysis (ref. [53]) suggests that PDHR can still provide its function without HPIS support for intact circuit faults which would improve the passivity of the system, but this is to be confirmed by the RP.
2. Based on the number of active systems required to support and initiate this system it is not a truly passive system, but once the cooling loops are established the system should continue to cool the reactor until the LUHS tanks run dry which is expected to take between one and three days depending on their configuration.
3. The PSA modelling carried out in Step 2 shows that the dominant failure mode for the system is RPS system failure, with the next failure mode more than two orders of magnitude less likely. The RPS platform has been assigned a probability of failure of 1 × 10-03/demand which is equal to the more reliable end of the typical reliability band assigned to a class 2 I&C system of 1 × 10-02 to 1 × 10-03. This failure probability includes both the hardware and software aspects of the RPS. I will follow this up in Step 3 to understand if the system modelling is representative and whether any reliability improvements can be made to this system, especially in the area of C&I.
4. Other failures include:

* CCF or independent failures of the HPIS pumps to start and run
* CCF of the MSIVs
* CCF of the PDHR heat exchangers (inside the LUHS tanks) due to tube blockages
* CCF of the PDHR hotleg outlet line SG Isolation Valves
* CCF of the SG blowdown containment isolation valves
* CCF of the ASD SG Control Valves failing to open on demand
* CCF of the refuelling pool filters due to blockage

1. The passive circulation parts of the system are not explicitly modelled in the PSA, apart from the heat exchanger tube blockages. This effectively means the RP are assuming PDHR is completely reliable once the initial valve movements have occurred. Substantiation of this will be required, primarily supported by RELAP and VIPRE modelling. The fault studies topic is leading on the assessment of these aspects. The RP may need to include further failure modes based on HAZID information for the ECCS, plus an additional failure mode to represent the uncertainty that the system will passively function. I will follow this up in Step 3.
2. It is notable that the inventory of the LUHS tanks and the refuelling pool water volume are required for both the ECCS and PDHR systems to function. Failure of the refuelling pool strainers could lead to failure of both the PDHR and ECC systems. These systems are claimed as separate protective measures on the fault schedule. The most risk significant CCF group in the PSA by Fussell Vesely importance is refuelling pool filter blockage. Because the LUHS tanks are simple and reliable stores of water the PSA does not highlight these as risk significant from a Fussell Vesely perspective, but they are risk significant from a Risk Increase Factor perspective.
3. To conclude, the RP have developed an adequate fault tree modelling methodology and adequate modelling of some front line SSCs. I am satisfied that the Step 2 PSA provides sufficient demonstration of the implementation of the methodology and insights into the risks arising from the front-line SSCs. There are shortfalls against the expectations for a full scope PSA in the areas of modelling of support systems and testing and maintenance, but the RP intend to address these in Step 3. Therefore I do not consider these shortfalls to be fundamental shortfalls for the Step 2 assessment. I will follow this up in Step 3.

### Data analysis

1. ONR expectations for data analysis are laid out in SAP FA.13 which notes that best-estimate methods and data should be used as far as possible within the PSA. Further guidance is available in Table A1-2.6 of NS-TAST-GD-030 on PSA (ref. [18]) and Section 5 of IAEA SSG-3 (ref. [21]).
2. The RP have developed a PSA Data Methodology (ref. [38]). The data methodology includes guidance on data assigned to initiating events, post fault component failures, common cause failures, operator actions and other data parameters required to support the PSA. The first issue of the methodology covers level 1 internal events at power in line with the PSA scope for Step 2. Having assessed the data methodology I am content that it sets out an approach in line with international RGP.
3. The data contained in the Step 2 PSA is described in the PSA Data Notebook (ref. [39]). I found discrepancies between the data methodology and the data notebook. Whilst the data methodology describes a range of secondary and tertiary data sources, the data notebook has only used NUREG/CR-6928 (ref. [54]) for individual components and US NRC CCF Parameter Estimates (ref. [55]) for CCFs. The RP note in the data notebook (ref. [39]) that the hierarchy of data sources to be employed when searching for data to assign to parameters has not generally been applied and most data has been sourced from NUREG/CR-6928 (ref. [54]) for historical consistency. While the PSA Data Notebook shows where each data point has been derived from, there is no justification for why NUREG/CR-6928 has been chosen over other sources beyond the fact that historically data has been sourced from NUREG/CR-6928. This represents a shortfall against RGP. The RP intend to improve the assignment of data as outlined in the introduction to the data notebook which I will follow up in Step 3.
4. The IEFs used in the PSA are taken from the Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies Report (ref. [29]) assessed in Section ‎4.2.1. It is notable that the RP have not developed any fault trees to derive initiating event frequencies for novel systems. This approach can be useful to model the effects of component failures causing an initiating event whilst also setting those components to a failed state in the mitigation systems in the PSA model. For IEFs that are not readily supported by international OPEX the RP should consider developing initiating fault trees.
5. The data assigned to CCFs in the PSA has been sourced from 'pooled' alpha factor parameters (for example all pumps, all motor operated valves etc, regardless of application) from CCF data published by INL. I consider this to be adequate for this stage of the project. The RP intend to use more component specific data when more information is available for their SSCs, though this is unlikely to be before operation.
6. The RP have used a 72-hour mission time for most components in the PSA model. This is in line with the design philosophy of the SMR which is intended to function without outside intervention for 72 hours. However, in many fault sequences the time required for an SSC to function will be significantly lower than 72 hours and the PSA is therefore using conservative reliability values for these components. The RP recognise this and intend to improve the modelling once further transient analysis is produced which defines when cold shutdown conditions are reached. I do not consider this to be a major source of conservatism as it is typical for PSAs to use a simplified set of mission times, with additional detail applied to particularly risk significant fault sequences where necessary.
7. The RP have not included any uncertainty parameters in the PSA model. This means that no uncertainty analysis has been carried out for Step 2. While this source of uncertainty is likely to be small compared to the larger uncertainties associated with missing scope and lack of transient analysis it represents a shortfall against UK RGP and is an aspect the RP should look to improve in the future. Conversely the RP have developed a substantial set of sensitivity analyses which are assessed in Section ‎4.2.9.
8. Overall, while the RP have developed a data methodology that meets RGP they have not yet applied it consistently to the PSA. I have identified potential shortfalls against UK RGP linked to the use of US data without justification and lack of uncertainty analysis and I will follow up in Step 3.

### Human Reliability Analysis

1. ONR expectations for human reliability analysis are laid out in SAP FA.13 on adequate representation which notes that PSA should include contributions to risk from pre-fault human errors (type A), human errors leading to faults (type B) and post-fault human errors (type C). SAP EHF.10 notes that Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety. Further guidance is available in Table A1-2.5 of NS-TAST-GD-030 on PSA (ref. [18]), NS-TAST-GD-063 on Human Reliability Analysis (HRA) (ref. [19]) and Section 5 of IAEA SSG-3 (ref. [21]).
2. The RP have produced a HBSC Modelling Methodology (ref. [36]) to lay out their approach to modelling operator actions in the PSA. The methodology only covers internal events at power in line with the scope of the PSA at Step 2. The RP have decided to embed the operator action basic events in the fault trees rather than having separate function events for them in the event trees. This leads to simpler event trees but means that it is less clear where operator actions are being claimed in the model. I have no concerns with this approach.
3. I assessed the HBSC Modelling Methodology to compare it against RGP. The RP intend to eventually include best-estimate analysis of Type A, B and C human errors. The PSA team are relying on the Human Factors (HF) team to maintain a database of HBSCs and to analyse dependencies, human machine interfaces (HMIs), accessibility and habitability of locations. The HBSC Modelling Methodology describes how operator actions will be modelled in the fault trees, but it does not discuss how human error probabilities will be calculated. This information is covered in the HRA Quantitative Assessment Strategy. This report does not define which technique will be used to derive human error probabilities (HEPs), instead it provides the analyst with a range of options including expert judgement and the human error assessment and reduction technique (HEART) and technique for human error rate prediction (THERP) methods and notes that these should be chosen on an event-by-event basis. It is not clear how a consistent set of HEPs can be developed on this basis.
4. The modelling of operator actions is reported in the PSA Operator Actions Modelling Report (ref. [37]). At this point in the project the RP have not identified any type A or type B human actions as they have not undertaken an exercise to identify them. The RP have identified a limited set of type C human actions. The process of developing the PSA has led to the identification of additional human actions that were not on the HBSC tracker held by the RP’s HF team. It is positive that the PSA can identify additional operator actions, but type A and B actions will need to be identified during Step 3.
5. While the Human Based Safety Claims Modelling Methodology (ref. [36]) adequately describes how the PSA will model operator actions, the RP’s PSA team are not responsible for quantifying the HEPs in the PSA model as this is the responsibility of the HF team. For Step 2 the RP have not carried out any task analysis or HRA due to a lack of data to derive best-estimate HEPs. This has led to them assigning all human error basic events in the PSA model the same HEP of 1 × 10‑02/demand on the basis that this represents a screening HEP.
6. Due to the use of this screening HEP some sequences in the PSA model have their risk significant exaggerated such as the ELOG fault which claims an operator action to top up the diesel generators within 72 hours. The results also show that only five operator actions cause a change in CDF depending on their reliability, indicating that the overall CDF for internal events at power is largely insensitive to HRA. This suggests that the RPs goal to minimise the need for operator reliability is being reflected by the PSA.
7. Use of a single HEP for all operator actions does not meet ONR expectations. More detailed analysis is required to enable the PSA to fulfil the claims made upon it. The PSA is also not modelling HMIs or local environment or transport routes which are shortfalls that cause the PSA to be optimistic. Maintenance activities are also not modelled in the PSA which is a potentially significant optimism. The RP intend to improve all these aspects during Step 3, and I will be following these up along with the HF inspector.
8. To conclude, the initial HRA shows that the Rolls-Royce SMR at power is not sensitive to human reliability. I have identified shortfalls against UK RGP for a full scope PSA, such as a lack of task analysis, lack of maintenance modelling and simplistic quantification of human errors. The RP have committed to making improvements in this area in Step 3 by producing HEPs using HEART (ref. [56]). Therefore I do not consider these to be fundamental shortfalls for Step 2 and I will follow this up in Step 3.

### Hazards analysis methodology

1. ONR expectations for PSA hazards analysis during GDA are set out in Table A1-2.7 of NS-TAST-GD-030 (ref. [18]) and Section 6 of IAEA SSG-30 (ref. [21]). It is expected that hazards analysis is undertaken for all hazards that are relevant to the design. ONR’s guidance to requesting parties (ref. [57]) also notes:

“That the RP’s submission should include a fully documented full scope PSA, including internal and external hazards”

“It is considered RGP that fully documented PSAs (in line with the PSA TAG) are provided for internal fire and flood, seismic and external flood with a level of detail in line with the level of development of the generic design.”

1. ONR also note in our GDA technical guidance (ref. [57]) that

“Partial scope PSA’s do not provide the full picture of the risk and distort the risk profile and importance of SSCs. Any decisions made with a partial scope PSA (such as design modifications) may not be optimal”

1. This latter guidance is relevant to the RP’s design.
2. The RP have set out their position in the PSA Hazard Event Modelling Methodology (ref. [40]). This document was originally to be accompanied by a hazards modelling report, but the RP moved that report into Step 3. Therefore, for Step 2 no hazards PSA modelling has been carried out. The RP note that previous GDA submissions have always had a reference design based on a plant that was significantly further along in development or had already been constructed elsewhere. This allowed previous RPs to use their reference designs to produce detailed hazard PSAs which require detailed information related to hazard curves and SSC designs. The RP’s design is a first of a fleet design and has no alternative reference facility. The RP also do not have a site identified. Whilst GDA is by its nature generic, previous GDAs have had a notional site identified that was used to inform some parameters of their site envelopes. This limits the availability of site-specific information which could inform hazards PSA.
3. I assessed the PSA Hazard Event Modelling Methodology and found that the RP have clearly set out the challenges and limitations related to information availability to carry out PSA hazards modelling. They have also set out a clear qualitative and quantitative screening process for hazards. The RP have been less clear about their plans for development of hazards PSA in Step 3. The RP have deferred almost all external hazards to the site licensing phase of the project. Only loss of offsite power and aircraft impact are expected to be covered in GDA. This leaves a large number of external hazards out of scope of GDA for the PSA. Conversely, all internal hazards are defined as being in scope for GDA. The RP’s intention is to develop quantitative bounding analyses for hazards to demonstrate that the numerical targets are met, but only minimal detail has been provided on how this will be carried out. Further information is expected early in Step 3 and this is an area I will be following up on.
4. To conclude, the RP have presented insufficient detail to form a judgement on the adequacy of the internal hazards analysis and I will seek further information in Step 3. For most external hazards, detailed analysis has been removed from the scope of GDA and additional evidence will need to be provided during site specific activities. For the external hazards remaining within GDA scope I will seek further information in Step 3.

### Quantification of PSA and interpretation of results

1. ONR expectations for use of PSA results are set out in SAP FA.10 on the need for PSA. The PSA should enable a judgement to be made of the acceptability or otherwise of the overall risks against numerical targets five to nine and should help to demonstrate that the risks are, and remain, ALARP. Further guidance is available in Table A1-2.9.2 of NS-TAST-GD-030 (ref. [18]) and Section 5 of IAEA SSG-3 (ref. [21]).
2. The PSA model has been developed in RiskSpectrum. This is an internationally recognised PSA code used by around 60% of the world’s nuclear power plants. Due to this pedigree I do not intend to seek verification and validation evidence for the RiskSpectrum software as I consider that the RP are using it within the typical operating parameters that other licensees use.
3. The RP have used the Step 2 PSA to produce a core damage frequency for internal events at power. The RP have not produced a large or early release frequency via a level 2 PSA or offsite consequence analyses via a level 3 PSA. The current scope of the PSA is sufficient to make a partial comparison against the RP’s own target for CDF but is not sufficient to enable a comparison against ONR’s numerical targets seven, eight and nine. To mitigate this the RP has produced the Assessment of Limitations Report which is assessed in Section ‎4.2.9.
4. The PSA Main Report (ref. [41]) shows that the CDF of the Step 2 PSA is 7.56 × 10-07/yr. This compares with the RPs CDF targets of (shall be less than) 1 × 10-05 /yr and (should be lower than) 1 × 10-07/yr. The Step 2 PSA does not include shutdown states or hazards which will increase the CDF when they are included. There is also likely to be additional risk contributions when maintenance and HVAC are added to the model and the electrical and C&I modelling are improved. The RPs assessment of limitations document (ref. [42]) reviews this CDF and assesses how it would be likely to change if the PSA modelling was improved and if the additional missing scope was added to the PSA. This is assessed in Section ‎4.2.9.
5. The CDF of 7.56 × 10-07 shows that the Step 2 PSA is not identifying any sequences leading to intolerable risk levels. The Step 2 PSA results suggest that the basic safety levels of ONR’s numerical targets seven, eight and nine should be capable of being met based on further design development and analysis being produced. However, there is the risk that a fault sequence linked to the areas out of scope of Step 2 of the PSA (for example, hazards, fuel route, shutdown states, level 2 PSA) could present a high risk when these aspects are modelled later in the project. The limited scope of the PSA must be considered when comparing against targets or results from other designs. The RP are intending to demonstrate that CDF is less than 1 × 10-07/yr during later stages of the project.
6. The most significant sequence in the PSA model, representing 33% of CDF, is a 168-hour ELOG followed by operator failure to top up the diesel tanks within 72 hours to ensure continued operation of the diesel generators. I consider that the operator action HEP of 1 × 10-02 is significantly conservative given the long timescales available and the simplicity of the action. The assumption that core damage would occur due to operator top‑up failure after 72 hours of post-trip cooling is also conservative as the PDHR and ECC systems can function without external power once they are aligned. However, this sequence has an IEF of 1 × 10-05 /year based on historical ONR guidance provided to a previous RP. Since that time the expected frequency of ELOG has increased. This was communicated by ONR to the RP in a letter (ref. [48]). The RP have indicated they will discuss the potential for more frequent loss of grid scenarios with National Grid but have not updated the IEF for ELOG in the latest PIE/IEF document (ref. [30]). It is likely that the RP will be able to demonstrate that their design can tolerate the ELOG duration specified in the letter without claiming any operator actions, but the RP need to demonstrate this which I will follow up in Step 3.
7. Many of the most risk significant sequences in the PSA are related to spurious actuation of systems. It is positive that the RP are modelling spurious initiation of systems at this stage of the project, but in some cases there is uncertainty as to what effect the spurious failures would have on the wider plant. Further C&I and transient analysis is required to support development of these sequences. I will follow this up in Step 3.
8. The PSA Main Report presents the key risk sequences and key minimal cutsets (MCS) for the level 1 PSA. The descriptions of the fault sequences are clear and easy to follow. I provided feedback to the RP on how they could improve the presentation of the PSA results, for example by including importance listings for individual component failures and by looking at risk increase factor in addition to Fussell Vesely importance. I noted that there is limited discussion of what the PSA is indicating about the design. This is related to the findings of RO-RRSMR-002 on PSA (ref. [50]) which will be addressed by the RP’s responses to Actions A3 and A4 (ref. [51]). The RP indicated they will address these comments when they produce the next version of the PSA Main Report. I will follow this up in Step 3.

#### C&I sensitivity

1. The RP have carried out C&I sensitivity analysis in their response to RQ‑01203 (ref. [43]). The study shows that the CDF is sensitive to the reliability of both the RPS and DPS systems. The RPS system has been assigned a reliability of 1 × 10-03 which is set at the reliable end of the typical band of reliability for Class 2 systems as described in NS-TAST-GD-046 (ref. [58]) on C&I. The DPS has been assigned a reliability of 1 × 10-04 which is the best reliability that can be claimed on a high confidence basis according to NS-TAST-GD-046.

**Table 2: C&I reliability and sensitivity**

|  | RPS | DPS |
| --- | --- | --- |
| Class | 2 | 1 |
| Typical Reliability for this Class | 1 × 10-02 – 1 × 10-03 | 1 × 10-03 – 1 × 10-05 |
| Assigned Reliability | 1 × 10-03 | 1 × 10-04 |
| CDF Sensitivity to 1 decade reduction | 2.38 | 2.04 |

1. I queried why the RP had chosen to use high reliability values when the typical approach by RPs is to use the lower end of the band. The RP noted that this is a historical choice of modelling, but it is one they intend to retain and justify during Step 3. It is notable that these are the values the RP are using for the deterministic case, these are not ‘best-estimate’ PSA-specific values. The sensitivity study showed that, based on the current simplified PSA modelling, changing the reliability values of the RPS and DPS to the lower end of their reliability bands would increase CDF by a factor of 12.7. To claim these reliabilities the RP will need to substantiate the system accordingly which will be followed up by the C&I inspector. The RP have also indicated that they intend to develop a best-estimate software reliability estimation framework The framework will be based on expert engineering judgement and will take account of category and classification of the equipment as well as any qualitative analyses that have been performed. I will work with the C&I inspector on the RPs justification of C&I reliability in the PSA in Step 3.

#### Undeveloped sequences

1. There are three sequences in the PSA model where the plant response strategy is still under development. The RP have identified these sequences with an UNDEVELOPED consequence. The frequency from these sequences does not contribute to the CDF. The three sequences are:

* Intermediate isolable LOCA (on failure of leak isolation) – This represents an unrecoverable loss of coolant outside of containment. Both PDHR and ECC require isolation of the primary circuit and containment respectively, and in this scenario isolation has failed. There is currently no analysis to support a claim on ECC without leak isolation, but further containment analysis work is planned by the RP to address this. I will follow this up in Step 3.
* Steam generator tube rupture (on failure to isolate the casualty steam generator) – This represents an unrecoverable loss of cooling outside containment. Like the point above, both PDHR and ECC require isolation to function. The containment analysis work planned by the RP will cover this scenario. I will follow this up in Step 3.
* Spurious initiation of HPIS (on failure of manual and automatic scram) – This represents a transient where no anti-reactivity is inserted into the core. The spurious HPIS initiation is assumed to prevent the use of ASF for boron injection. The initial transient of spurious HPIS initiation is unlikely to cause a significant reactivity transient so this fault should have large grace times to rectify the fault. I will follow this up in Step 3.

1. These sequences have a frequency of 1.4 x 10-5 in the PSA. If they were to lead to doses >1000mSv offsite this would put the risk between the BSO and BSL of numerical target 8. The RP will need to demonstrate during Step 3 that these sequences can be tolerated by the design of the plant or they will need to change the consequence to core damage.
2. I support the use of the UNDEVELOPED consequence as it allows the PSA to highlight areas of significant design uncertainty without further skewing the results of the PSA. If these sequences had been assigned the normal core damage consequence they would have dominated the results.
3. To conclude, the RP’s quantification of the PSA and interpretation of the PSA results that has been submitted is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence. However, due to the limited scope of the PSA at Step 2, no direct comparisons against ONR’s numerical targets can be made at this stage. I will seek further information in Step 3 to enable comparisons against the targets.

### Assumptions and limitations of the PSA

1. ONR’s expectations for assumptions management is outlined in SAP FA.11 on validity of PSA to note that assumptions used in the absence of design information should be justified and careful consideration taken of their impact on the analysis. SAP FA.13 on adequate representation of PSA notes that the sensitivity of the results to assumptions should be established. Further detailed expectations are set out in Table A1-1.5 of NS-TAST-GD-030 (ref. [18]).
2. The RP have made many assumptions during the production of the Step 2 PSA. The RP’s process for managing assumptions is captured in appendix B of the Event Sequence Modelling Report (ref. [33]). Assumptions are used to provide information to PSA analysts where there is a lack of input data or where a modelling simplification is being made. Each assumption is written up as an embedded table in the relevant modelling document to capture the ‘what, how, why, where and impact’ of the assumption on the PSA model. I consider that this approach is a robust way of identifying assumptions. It helps to make them clear to the reader, but it also forces the analyst to consider the impact of each assumption being made and to seek advice from the wider project where necessary. The totality of assumptions across the PSA are captured in the PSA assumptions log (ref. [59]). This is a live document which is submitted periodically to ONR to capture updates. The Step 2 assumptions log captures two hundred assumptions. This number will continue to grow as the project progresses and the RP will need to develop a process to manage the assumptions and identify which other disciplines are required to help close them out.
3. As noted in the previous sections, the Step 2 PSA has many limitations, related to scope, level of detail and availability of information from the wider project. The RP have also made a large number of potentially significant assumptions. The RP have recognised these limitations when compared with their own PSA Technical Requirements (ref. [27]) by producing an Assessment Of Limitations (AOL) report (ref. [42]). The AOL ranks the limitations into major, moderate and minor categories based on the significance of the limitation compared to the PSA technical requirements.
4. The RP have used information from PSAs submitted for previous GDAs (the HPR1000, EPR and AP1000) to estimate the typical risk associated with various aspects of light water reactor design. At this stage of the project this approach is practical and allows comparisons to be made. I noted to the RP that these GDA PSAs also have substantial limitations, and it would be preferable to refer to published modern standards PSAs for operating facilities rather than those from previous GDAs. The RP have calculated the proportion of risk associated with missing scope such as shutdown faults and then multiplied that proportion by the CDF from the Step 2 PSA. I consider this to be a better approach than using the absolute values from the different PSAs as it is generally not meaningful to directly compare the numerical values from different PSA models.
5. The limitations associated with the largest estimated changes in CDF are:

* Addition of shutdown faults for the reactor – 31% of CDF
* Addition of internal fire and flood hazards – 67% of CDF

1. These values would indicate a total CDF of around 1.5 × 10-06/yr. While there is substantial uncertainty around these values, they give an indication that the basic safety levels of ONR’s numerical targets seven, eight and nine should be capable of being met assuming continued development of the design and a robust containment strategy to manage severe accidents. However, there is the risk that a fault sequence linked to the areas out of scope of Step 2 of the PSA (for example hazards, fuel route, shutdown states, level 2 PSA) could present a high risk when these aspects are modelled later in the project.
2. The RP have quantified a number of other assumptions and carried out a dominant sequence review to establish if any of the most risk significant sequences should have their frequencies revised. The total CDF resulting from all recalculations is 3.44 × 10-07/yr. While I do not agree with every numerical change made, the process the RP has followed adds value to the PSA. This is because it shows that the RP are using the risk insights from the PSA to understand where there are optimisms or conservatisms in their analysis. While the current PSA has substantial limitations the process followed here will help the RP to reduce risks as more details are added to the PSA.
3. There are also a substantial number of limitations where a numerical estimate cannot be performed or the PSA is insensitive to changes. Most limitations have a solution identified within the scope of GDA. I consider that the AOL is comprehensive and shows that the RP understand the limitations inherent in the PSA.
4. The limitations present in the Step 2 PSA mean that there are key topics that PSA is not able to inform at this time, despite my Assessment Plan (ref. [11]) indicating I would target certain matters. These include the lack of level 2 PSA modelling which means that no PSA insights are available for the design of containment or the SSCs designed to mitigate a severe accident. Similarly the lack of hazards information means that no PSA insights are available for the generic site envelope or the compact layout of the plant.
5. To conclude, I consider the RPs management of assumptions and limitations is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence.

### ALARP

1. ONR’s expectations regarding demonstration of risks being ALARP are set out in SAP FA.14 which states that the PSA should be used to support the demonstration that risks are tolerable and ALARP. I have also referred to NS-TAST0GD-005 which provides guidance on the demonstration of ALARP (ref. [17]).
2. As noted in Section ‎4.2.2 I raised RO-RRSMR-002 partly because Issue 1 of the PSA development strategy did not explain how the PSA would be integrated into the design and safety case. While the RP has produced a resolution plan and begun to submit documents, the actions associated with closing out these aspects have not been closed out at this time.
3. The PSA Main Report (ref. [41]) and Assessment Of Limitations (ref. [42]) contain no discussion of whether the PSA has demonstrated risks are ALARP which is a significant omission. The RP have not attempted to compare the results from the PSA against ONR’s numerical targets seven, eight and nine. I will follow up how the PSA will used to inform, complement, support and strengthen the demonstrations across the safety case that radiological risks have been reduced ALARP in the design as part of closing out RO-RRSMR-002.
4. The RP has also produced a standalone ALARP Summary Report (ref. [28]) which will inform E3S chapter 24 on ALARP. The report is based on the RD7 design reference from November 2023. The project has a decision record template which includes key design objectives related to PSA, for example aiming to achieve a core damage frequency of 1 × 10‑06/yr but targeting 1 × 10‑07/yr. I have not sampled any decision records at this stage, but I expect to do so in Step 3 or as part of the closeout of the PSA RO-002.
5. The ALARP report recognises the fact that LUHS inventory, MSIVs and the refuelling pool volume are all common elements between PDHR and ECC. The report does not describe the potential for the refuelling pool strainers to block due to a common cause leading to the failure of both systems. The report notes that the RP did consider having separate LUHS tanks for PDHR and ECC and concluded that the benefits were grossly disproportionate to the disbenefits. The Step 2 PSA results support this conclusion.
6. The report notes that PSA has been used to risk inform the design of the MSIVs and ASD system. This work has not been submitted for assessment by ONR.
7. The ALARP report discusses the design development of the containment and in-vessel retention systems. However, due to the lack of level 2 PSA modelling in Step 2 the PSA cannot provide any insights for the design of containment or severe accidents systems at this time. This will be addressed during Step 3, and I will follow up this area.
8. Overall the ALARP report indicates that the RP has been cognisant of ALARP throughout the design process. I consider that there is significant work for the RP to do to demonstrate that the risks from the design are ALARP. The RP need to demonstrate how the PSA is risk informing the design and the E3S case. I will follow this up in Step 3 as part of closure of RO-RRSMR-002.

# Conclusions

## Conclusions

1. This report presents the Step 2 PSA 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 found that the tier 1 chapters and tier 2 and 3 submissions were consistent with each other. I targeted my assessment, in accordance with my assessment plan (ref. [11]), at the content of most relevance to PSA 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:

* In general the RP have produced methodology documents that apply standards and techniques that are recognised as RGP for PSA. However in many cases these methodologies have not yet been fully applied and therefore there are limitations and gaps in various aspects of the PSA.
* The RP has developed an appropriate approach for the identification of initiating events and derivation of best-estimate IEFs for at-power faults. However, at this stage in the development of the design and safety case the RP has not identified all potential initiating faults and their associated IEFs. I consider that the information that has been submitted to date is consistent with RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence in the future.
* Regarding the scope and development of the PSA, the RP has developed a set of PSA Technical Requirements in line with UK and international RGP. However, I have found shortfalls in the PSA Development Strategy. These shortfalls were linked to planning for adding the missing scope of the PSA, quality assurance and demonstrating how PSA is used to risk inform the safety case and design. I raised regulatory observation RO-RRSMR-002 and accepted a resolution plan from the RP. The RP have submitted initial documents to begin addressing the RO. I will follow up the closure of this RO in Step 3.
* Regarding event tree modelling and accident sequence analysis, the RP has produced a methodology for Step 2 in line with UK and international RGP. The RP have modelled accident sequences based on the design intent of the SSCs. Currently there is insufficient transient analysis and radiological consequence analysis to define the effects of accident sequences on the reactor core and wider plant. I will follow up this aspect in Step 3.
* Regarding fault tree modelling and the representation of passive systems, the RP has produced a methodology for Step 2 in line with UK and international RGP and have developed adequate modelling of some front line SSCs. I have identified shortfalls against UK RGP for a full scope PSA related to modelling of support systems and testing and maintenance which the RP intend to address in Step 3. Therefore I do not consider these shortfalls to be fundamental shortfalls for the Step 2 assessment. I will follow up these aspects in Step 3.
* Regarding the use of data in the PSA model, while the RP have developed a data methodology that meets RGP they have not yet applied it consistently to the PSA. I have identified potential shortfalls against UK RGP linked to the use of US data without justification and lack of uncertainty analysis and I will follow up in Step 3.
* Regarding the HRA, there is a significant amount of work required by the RP to identify all relevant operator actions and quantify them using appropriate techniques. At this stage a single screening value has been assigned to all operator actions which skews the results of the PSA. This represents a shortfall against UK RGP for a full scope PSA. There is a lack of task analysis, lack of maintenance modelling and simplistic quantification of human errors. I do not consider these to be fundamental shortfalls for Step 2 as the RP have committed to improving these aspects and I will follow this up in Step 3.
* Regarding the hazards PSA, the RP have presented insufficient detail to form a judgement on the adequacy of the internal hazards analyses and I will seek further information in Step 3. For external hazards, detailed analysis has been removed from the scope of GDA for most external hazards and additional evidence will need to be provided during site specific activities. For the external hazards remaining within GDA scope I will seek further information in Step 3.
* Regarding the quantification of the PSA and results, the RP has presented an adequate first issue of the PSA Main Report. Due to the limited scope of the PSA at Step 2, no direct comparisons against ONR’s numerical targets can be made at this stage. The Step 2 PSA results suggest that the basic safety levels of ONR’s numerical targets 7, 8 and 9 should be capable of being met based on further design development and analysis being produced. However, there is the risk that a fault sequence linked to the areas out of scope of Step 2 of the PSA (for example, hazards, fuel route, shutdown states, level 2 PSA) could present a high risk when these aspects are modelled later in the project. I will seek further information in Step 3 to enable comparisons against the numerical targets.
* Regarding the assumptions and limitations in the PSA, the RP have developed a robust process for tracking assumptions in the PSA. They have used this to develop a comprehensive assessment of limitations. I consider that this approach is consistent with UK RGP and should enable the RP to further develop the generic Rolls-Royce SMR design and associated E3S case evidence.
* Regarding demonstration that risks are ALARP, the PSA documentation seen so far has limited discussion on this topic. As part of closing out RO-RRSMR-002 the RP will have to demonstrate how the PSA has been used to inform the design and the safety case. I will follow up closure of the RO in Step 3.

1. Overall, based on my assessment to date of the limited scope PSA, 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.

## Recommendation

1. My recommendation is 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, E3S Case Version 2, Tier 1, Chapter 1: Introduction, SMR0004294, Issue 3, May 2024. (Record ref. ONRW-2019369590-9881). |
| [2] | Rolls-Royce SMR Limited, E3S Case Version 2, Tier 1, Chapter 7: Instrumentation and Control, SMR0003929, Issue 3, May 2024. (Record ref. ONRW-2019369590-9887). |
| [3] | Rolls-Royce SMR Limited, E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis, SMR0003977, Issue 3, May 2024. (Record ref. ONRW-2019369590-9923). |
| [4] | Rolls-Royce SMR Limited, E3S Case Version 2, Tier 1, Chapter 18: Human Factors Engineering, SMR0004520, Issue 3, May 2024. (Record ref. ONRW-2019369590-9908). |
| [5] | Rolls-Royce SMR Limited, E3S Case Version 2, Tier 1, Chapter 24: ALARP Summary, SMR0004487, Issue 2, May 2024. (Record ref. ONRW-2019369590-9914). |
| [6] | 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. |
| [7] | ONR, Safety Assessment Principles for Nuclear Facilities (SAPs), 2014 Edition, Revision 1, January 2020. www.onr.org.uk/media/pobf24xm/saps2014.pdf. |
| [8] | ONR, Technical Assessment Guides. www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/technical-assessment-guides-tags/nuclear-safety-tags/technical-assessment-guide. |
| [9] | ONR, Guidance on the Production of Reports for Permissioning and Assessment, NS-TAST-GD-108, Issue No. 1, December 2022. (Record 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 PSA Assessment Plan for the Generic Design Assessment of the Rolls-Royce SMR, ONR-GDA-AP-22-021, Issue No. 1, March 2023. (Record ref. ONRW-2126615823-391). |
| [12] | ONR, Generic Design Assessment of the Rolls-Royce SMR Step 2 Summary, Issue 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-2019369590-8058). |
| [14] | IAEA, Safety Standards. www.iaea.org. |
| [15] | WENRA, WENRA Safety Reference Levels for Existing Reactors 2020. February 2021. WENRA. www.wenra.eu. |
| [16] | 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. |
| [17] | ONR, Regulating Duties to Reduce Risks to ALARP (As Low As Reasonably Practicable), NS-TAST-GD-005, Issue 12, January 2024. www.onr.org.uk/media/documents/guidance/ns-tast-gd-005.docx. |
| [18] | ONR, Probabilistic Safety Analysis, NS-TAST-GD-030, Revision 7, June 2019. www.onr.org.uk/media/msjpkl10/ns-tast-gd-030.pdf. |
| [19] | ONR, Human Reliability Analysis, NS-TAST-GD-063, Issue 6, December 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-063.docx. |
| [20] | IAEA, Format and Content of the Safety Analsyis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61, September 2021. www.iaea.org. |
| [21] | IAEA, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, March 2024. www.iaea.org. |
| [22] | IAEA, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) For Applications In Nuclear Power Plants, IAEA-TECDOC-1804, October 2016. www.iaea.org. |
| [23] | Rolls-Royce SMR Limited, GDA Design Reference Report, SMR0009043, Issue 2, April 2024. (Record ref. ONRW-2019369590-8872). |
| [24] | Rolls-Royce SMR Limited, Fault Schedule (Version 6), SMR0004444, Issue 1, March 2023. (Record ref. ONRW-2019369590-2659). |
| [25] | Rolls-Royce SMR Limited, Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies, SMR0001389, Issue 3, April 2023. (Record ref. ONRW-2019369590-2657). |
| [26] | Rolls-Royce SMR Limited, E3S Case CAE Routemap. (Record ref. ONRW-2126615823-1777). |
| [27] | Rolls-Royce SMR Limited, PSA Technical Requirements, SMR0004734, Issue 2, January 2024. (Record Ref. ONRW-2019369590-2666). |
| [28] | Rolls-Royce SMR Limited, ALARP Summary Report, SMR0009086, Issue 1, January 2024. (Record ref. ONRW-2019369590-6729). |
| [29] | Rolls-Royce SMR Limited, Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies, SMR0001389, Issue 2, January 2023. (Record ref. ONRW-2019369590-2656). |
| [30] | Rolls-Royce SMR Limited, Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies, SMR0001389, Issue 4, January 2024. (Record ref. ONRW-2019369590-7003). |
| [31] | Rolls-Royce SMR Limited, PSA Development Strategy, SMR0004735, Issue 2, January 2024. (Record ref. ONRW-2019369590-6086). |
| [32] | Rolls-Royce SMR Limited, Event Sequence Modelling Methodology, SMR0005508, Issue 1, April 2023. (Record ref. ONRW-2019369590-2668). |
| [33] | Rolls-Royce SMR Limited, PSA Event Sequence Modelling Report, SMR0008247, Issue 1, October 2023. (Record ref. ONRW-2019369590-4507). |
| [34] | Rolls-Royce SMR Limited, PSA SSC Modelling Methodology, SMR0006323, Issue 1, June 2023, (Record ref. ONRW-2019369590-3254). |
| [35] | Rolls-Royce SMR Limited, PSA SSC Modelling Report, SMR0008526, Issue 1, October 2023. (Record ref. ONRW-2019369590-4893). |
| [36] | Rolls-Royce SMR Limited, PSA Human Based Safety Claims Modelling Methodology, SMR0006322, Issue 1, June 2023. (Record ref. ONRW-2019369590-3253). |
| [37] | Rolls-Royce SMR Limited, PSA Operator Actions Modelling Report, SMR0008148, Issue 1, October 2023. (Record ref. ONRW-2019369590-4506). |
| [38] | Rolls-Royce SMR Limited, PSA Data Methodology, SMR0006379, Issue 1, June 2023. (Record ref. ONRW-2019369590-3253). |
| [39] | Rolls-Royce SMR Limited, PSA Data Notebook, SMR0007938, Issue 1, October 2023. (Record ref. ONRW-2019369590-4890). |
| [40] | Rolls-Royce SMR Limited, PSA Hazard Event Modelling Methodology - SMR0008733, Issue 1, December 2023. (Record ref. ONRW-2019369590-5809). |
| [41] | Rolls-Royce SMR Limited, PSA Main Report, SMR0008850, Issue 1, January 2024. (Record ref. ONRW-2019369590-6335). |
| [42] | Rolls-Royce SMR Limited, PSA Assessment of Limitations, SMR0008732, Issue 1, January 2024. (Record ref.ONRW-2019369590-6334). |
| [43] | ONR, Schedule of Step 2 Regulatory Queries, April 2024. (Record ref. ONRW-2019369590-9071). |
| [44] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Fault Studies, ONRW-2126615823-2793, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2793). |
| [45] | U.S. Nuclear Regulatory Commission, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995, NUREG/CR-5750, 1999. www.nrc.gov. |
| [46] | Idaho National Laboratory, Initiating Event Rates at U.S. Nuclear Power Plants, 2020 Update, November 2021, INL/EXT-21-63577. www.nrcoe.inl.gov. |
| [47] | ONR, Regulatory Observation - Analysis of loss of offsite power event, RO-ABWR-0009, July 2014. www.onr.org.uk/media/gvtlyuu0/ro-abwr-0009.pdf. |
| [48] | ONR, letter to Rolls-Royce SMR Ltd, Information on Extended Loss of Grid scenarios, RRSMR-REG-0017N, May 2023. (Record ref. ONRW-2019369590-2482). |
| [49] | Rolls-Royce SMR Limited, PSA Development Strategy, SMR0004735, Issue 1, March 2023. (Record ref. ONRW-2019369590-2669). |
| [50] | ONR, Regulatory Observation - PSA Project Plan and Integration, RO-RRSMR-002, Revision 0, August 2023. www.onr.org.uk/media/2gupvfgm/ro-rrsmr-002.docx. |
| [51] | Rolls-Royce SMR Limited, Rolls-Royce SMR RO Resolution Plan, RO-RRSMR-002, PSA Project Plan and Integration, SMR0008157, Issue 1, November 2023. www.onr.org.uk/media/l0enb10z/ro-rrsmr-002-plan.docx. |
| [52] | Rolls-Royce SMR Limited, PSA Technical Requirements, SMR0004734, Issue 2, January 2024. (Record ref. ONRW-2019369590-2666). |
| [53] | Rolls-Royce SMR Limited, Reactor Plant Performance Fault Study Analysis Summary, SMR0007538, Issue 1, November 2023. (Record ref. ONRW-2019369590-5147). |
| [54] | Idaho National Laboratory, Industry-Average Performance for Components and Initiating Events at U.S Commercial Nuclear Power Plants, NUREG/CR-6928 (3rd Update 2020), 2021. www.nrcoe.inl.gov. |
| [55] | Idaho National Laboratory, CCF Parameter Estimations 2020 Update, INL/EXT-21-62940, 2022. www.nrcoe.inl.gov. |
| [56] | ONR, RR SMR GDA – PSA Level 4 Meeting 15 (Joint with HF) – Human Reliability Analysis, ONR-NR-CR-24-064, May 2024. (Record ref. ONRW-2019369590-9442). |
| [57] | ONR, New Nuclear Power Plants GDA Technical Guidance, ONR-GDA-GD-007, Revision 0, May 2019. www.onr.org.uk/media/c2delysl/onr-gda-007.pdf. |
| [58] | ONR, Computer Based Safety Systems, NS-TAST-GD-046, Issue 7, December 2023. www.onr.org.uk/media/documents/guidance/ns-tast-gd-046.docx. |
| [59] | Rolls-Royce SMR Limited, PSA Assumptions Log, SMR0008567, Issue 1, October 2023. (Record ref. ONRW-2019369590-4891). |
| [60] | ONR, Agreement of Resolution Plan for RO-RRSMR-002 – PSA Project Plan and Integration, November 2023. (Record ref. ONRW-2126615823-1672). |

# Appendix 1 – Relevant SAPs considered during the assessment

|  |  |  |
| --- | --- | --- |
| SAP No. | SAP Title | SAP Text |
| FA.1 | Design basis analysis, PSA and severe accident analysis | Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP. |
| FA.10 | Need for PSA | Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis. |
| FA.11 | Validity | PSA should reflect the current design and operation of the facility or site. |
| FA.12 | Scope and Extent | PSA should cover all significant sources of radioactivity, all permitted operating states and all relevant initiating faults. |
| FA.13 | Adequate Representation | The PSA model should provide an adequate representation of the facility and/or site. |
| FA.14 | Use of PSA | PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities. |

1. The ‘first’ protective safety function refers to the defence in depth level 3 protective safety function which is demanded first chronologically, rather than the ‘principal’ safety function which is delivered by class 1 SSCs. [↑](#footnote-ref-2)
2. The ‘second’ protective safety function refers to the defence in depth level 3 protective safety function which is demanded second chronologically. [↑](#footnote-ref-3)
3. The first value corresponds to ‘shall be lower than’ and the second value corresponds to ‘should be lower than’. [↑](#footnote-ref-4)