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



ONR Assessment Report

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

**Report Title**: Step 2 assessment of Security

**Authored by**: [Redacted]

**Report Issue No**: 1

**Document ID**: ONRW-2126615823-3520

**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 security 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 security case, and the suitability of the methodologies, approaches, codes, standards and philosophies which form the building blocks for the design and generic safety and security cases.

I targeted my assessment, in accordance with my assessment plan, at the content of most relevance to security against the expectations of ONR’s Security Assessment Principles (SyAPs), 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:

* The Generic Security Report (GSR) that provides a framework for a security case.
* Their overarching security philosophy based on a Secure by Design (SbD) approach that sought, through threat analysis, to identify and mitigate the security risks within the design.
* Thereafter, I targeted their risk methodologies and application (in their case via trials) for sabotage, theft and cyber security.
* Given the design’s maturity, I did not seek a detailed description of their developing Physical Protection System (PPS) and Cyber Protection System (CPS). However, I targeted their framework for developing protection against identified and quantified risks within the context of developing a future security plan.

Based upon my assessment, I have concluded the following:

* I judge that the GSR provides a comprehensive framework on which to build on in Step 3. The RP has adopted an ambitious approach to developing a security case. The security case is integrated into a wider E3S case and their innovative approach to SbD offers ways to influence the design for security benefit.
* Their security ‘narrative’ is an intelligent one that reflects a SyAPs based approach. The RP’s overall security case development also seeks to integrate cyber security into wider security risk management and reaches outside security especially to Control and Instrumentation.
* The RP has focused correctly on identifying risks to the design. While design maturity has been a limiting factor, the RP has developed workable methodologies for determining and managing security risks.
* The RP has met the intended Vital Area Identification & Categorisation objectives for Step 2. It has developed a set of arrangements which I consider to have demonstrated satisfactory alignment with RGP. The design maturity has limited the availability of the design data to enable a complete and comprehensive demonstration of the RP’s arrangements at this time. In addition, the RP must ensure it uses the UK Design Basis Threat (DBT) in Step 3.
* The RP has met the intended cyber security objectives for Step 2. They have improved their methodology and sought to apply it at an early stage of design maturity. While I expected to see a more complete demonstration of the methodology, and there are aspects which will require further improvement, the RP has provided a good foundation for Step 3.
* The RP’s Integrated Security Solution (ISS), which includes the PPS and CPS, has provided me with a valuable picture of what the RP aims to achieve in GDA and what aspects of the security regime will become the responsibility of the eventual licensee. With a design still in development, further and ongoing risk analysis against sabotage and theft, with other malicious actions, will be necessary. The ISS will need to be sufficiently detailed to inform security systems requirements.

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

# List of Abbreviations

ARF Airborne Release Fraction

ATT&CK Adversary Techniques, Tactics and Common Knowledge

CBSIS Computer-based System Important to Safety

CBSy Computer-based Security System

C&I Control and Instrumentation

CNSS Civil Nuclear Security and Safeguards (ONR)

CPS Cyber Protection System

CS&IA Cyber Security and Information Assurance

CSR Cyber Security Report

CSRAM Cyber Security Risk Assessment Methodology

DAC Design Acceptance Confirmation

DBT Design Basis Threat

DESNZ Department for Energy Security and Net Zero

DF Decontamination Factor

DiD Defence in Depth

DPS Diverse Protection System

E3S Environment, Safety, Security and Safeguards

FAB Spent Fuel Storage & Cask Cooling System

FS Fault Schedule

FSF Fundamental Safety Function

FSyP Fundamental Security Principle

GDA Generic Design Assessment

IAEA International Atomic Energy Agency

ICS Industrial Control System

IEC International Electrotechnical Commission

IET Institution of Engineering and Technology

IEMO Initiating Event of Malicious Origin

ISS Integrated Security Solution

IT Information Technology

KSyPP Key Security Plan Principle

NPP Nuclear Power Plant

NSSP Nuclear Site Security Plan

ONR Office for Nuclear Regulation

OT Operational Technology

PIE Postulated Initiating Events

PSEP Potential Sabotage Event Scenario

PSA Probabilistic Safety Analysis

PPS Physical Protective Security

PWR Pressurised Water Reactor

RGP Relevant Good Practice

RP Requesting Party

RPS Reactor Protection System

RQ Regulatory Query

SbD Secure by Design

SES Sabotage End State

SME Subject Matter Expert

SMR Small Modular Reactor

SFPCS Spent Fuel Pool Cooling System

STIX Structured Threat Information Expression

SyAPs Security Assessment Principles

SSC Structure, System and Component

TAG Technical Assessment Guide(s) (ONR)

TSC Technical Support Contractor

URC Unacceptable Radiological Consequence

UK DBT UK Design Basis Threat

VA Vital Area

VAI&C Vital Area Identification & Categorisation

Contents

[Executive Summary 3](#_Toc172735016)

[List of Abbreviations 5](#_Toc172735017)

[1. Introduction 8](#_Toc172735018)

[2. Assessment standards and interfaces 10](#_Toc172735019)

[3. Requesting party’s submission 14](#_Toc172735020)

[4. ONR assessment 19](#_Toc172735021)

[5. Conclusions 50](#_Toc172735022)

[References 52](#_Toc172735023)

[Appendix 1 – Relevant SyAPs and SAPs considered during the assessment 58](#_Toc172735024)

# Introduction

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

## Background

1. The ONR’s GDA process (ref. [8]) 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 Security (ref. [9]). 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. [10]).
   1. Scope
6. 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.
7. The overall scope of the Rolls-Royce SMR GDA is described in (ref. [11]). Rolls-Royce SMR Limited has indicated that it intends to complete a three step GDA, with the objective of receiving a DAC from ONR and have aligned their GDA scope with this objective. The GDA scope defines the generic plant and layout and includes all systems, structures and components that are identified as being important to safety, security and safeguards, all modes of operation, and all stages of the plant lifecycle.
8. However, given the step-wise assessment during GDA, information has not been submitted for all aspects within the GDA scope during Step 2 (ref. [12]). The following aspects of the E3S case are therefore out of scope of this assessment:

* Enterprise Information Technology (IT) network but not the security enforcing interfaces with Operational Technology (OT);
* Internet facing conduits.

1. My assessment has considered the following aspects of the RP’s case:

* The scope, structure and content of the security case consistent with Relevant Good Practice (RGP);
* The application of security principles drawing from SyAPs with an emphasis of Key Security Plan Principles (KSyPPs) and categorisation of risk within the design;
* Risk analysis approaches and methodologies using the UK Design Basis Threat (UK DBT);
* The application of risk methodologies to show efficacy against SyAPs expectations; and,
* The security case framework that provides a ‘golden thread’ from risk analysis to a protective security regime sufficient to inform a licencee thereby meeting regulatory expectations.

# 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 Security Assessment Principles (SyAPs) (ref. [5]) and Safety Assessment Principles (SAPs) (ref. [13]) constitute the regulatory principles against which the RP’s case is judged. Consequently, the SyAPs and 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]) and nuclear security series (ref. [15]) 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. The relevant SyAPs, SAPs and IAEA standards are embodied and expanded on in the TAGs (ref. [6]). The TAGs provide the principal means for assessing the security aspects in practice.

### Security Assessment Principles (SyAPs)

1. The main SyAPs applied within my assessment are Fundamental Security Principles (FSyPs) 6 and 7 and KSyPP 1-5 and 7.
2. KSyPP 1-5 and 7 covering SbD, the threat, graded approach, defence in depth, security categorisation and classification and codes and standards were used throughout the assessment. These principles, and related guidance, that inform security case design were used to assess all the RP’s submissions.
3. FSyP 6 and 7 provided the guidance on the assessment of the RP’s submissions on the categorisation for sabotage, theft and their structure for describing a protection system designed in sufficient detail to be developed further in Step 3.
4. A list of the SyAPs used in this assessment is recorded in Appendix 1.

### Safety Assessment Principles for Security

1. Given the complementary relationship between safety and security, ONR SAPs include guidance on how to assess security related matters where these fall within the vires of safety legislation i.e., because of overlap or inter-relationship. Where SAPs are applied as part of this assessment a justification has been provided.
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:

* CNSS-TAST-GD-11.1 - Guidance on the Security Assessment of Generic New Reactor Designs (ref. [16])
* CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management (ref. [17])
* CNS-TAST-GD-7.3 - Protection of Nuclear Technology and Operations (ref. [18])
* CNS-TAST-GD-6.1 - Categorisation for Theft (ref. ( [19])
* CNS-TAST-GD-6.2 - Categorisation for Sabotage (ref. [20])
* NS-TAST-GD-045 - Radiological analysis - Fault conditions (ref. [21])
* CNS-TAST-GD-6.3 - Physical Protection System Design (ref. [22])
* CNS-TAST-GD-11.4.1- Secure by Design (ref. [23])

### National and international standards and guidance

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

* UK Design Basis Threat (DBT) (ref. [24])
* IAEA, Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC/225/Revision 5 (ref. [25])
* IAEA, Identification of Vital Areas at Nuclear Facilities, Nuclear Security Series No. 16 (ref. [26])
* IAEA, Computer Security Techniques for Nuclear Facilities, Nuclear Security Series No. 17-T (ref. [27])
* IAEA, Engineering Safety aspects of the Protection of Nuclear Power Plants against Sabotage, Nuclear Security Series No. 4 (ref. [28])
* IAEA, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Nuclear Security Series No. 33-T (ref. [29])
* IAEA, Handbook on the Design of Physical Security Protection Systems for Nuclear Material and Facilities, Nuclear Security Series No. 40-T (ref. [30])
* IAEA, Insider Threats, Nuclear Security Series No. 8-G (ref. [31])
* IET, Code of Practice: Cyber Security and Safety, 2021 (ref. [32])
* BS ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks (ref. [33])
* BS EN IEC 62443-3-2:2021 Security for Industrial Automation and Control Systems Part 3-2: Security risk assessment for system design (ref. [34])
* BS EN IEC 62443-3-3:2019 Industrial communication networks – Network and System Security Part 3-3: system security requirements and security levels (ref. [35])
* BS EN IEC 62645:2020 Nuclear power plants - Instrumentation, Control and Electrical Systems - Cybersecurity requirements (ref. [36])
* BS EN IEC 62859:2020 Nuclear power plants - Instrumentation and control systems - requirements for coordinating Safety and Cybersecurity (ref. [37])

## Integration with other assessment topics

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

* Cyber security and C&I where C&I provided input to the assessment of the RP’s submissions in relation to CBSIS (ref. [38]);
* Internal hazards for discussion around maliciously initiated Type 1 DBT events (ref. [39]);
* Fault studies for advice on the maturity of the safety analysis used to inform Vital Area Identification and Categorisation (VAI&C) (ref. [40]);
* Probabilistic Safety Analysis (PSA) for advice on the maturity of the safety analysis used to inform VAI&C (ref. [41]);
* Radiation protection for advice on dose consequence modelling (ref. [42]);
* Fire safety regarding deconfliction between emergency arrangements and security access management (ref. [43]); and
* Electrical engineering regarding power supplies to anticipated security systems (ref. [44]).

## Use of technical support contractors

1. During Step 2 I have not engaged Technical Support Contractors (TSCs) to support my assessment of the security 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 security case. It also identifies the documents submitted by the RP which have formed the basis of my security 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 MTh) 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 security features, by way of systems and components that will meet regulatory expectations for protection of the plant, are not part of the early design. Security risks from sabotage of the plant and theft of nuclear material will only become apparent once the design has matured.

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

1. The structure of the E3S case largely aligns with the IAEA guidance for safety cases, SSG-61 (ref. [45]), supplemented to include UK specific expectations and expanded to include the other E3S purposes including security.

## Summary of the requesting party’s E3S case for Security

1. The aspects covered by the Rolls-Royce SMR security case can be broadly grouped under several headings. These topics are reflected in the RP’s claims summarised in the GSR Issue 3 (ref. [3]). In brief they are:

### Generic Security Report

1. The RP submitted both a GSR at Issue 1 (ref. [46]) and a strategy for its development (ref. [47]) early in this step. Both documents, at Tier 1, build on the Step 1 Preliminary Security Report. However, I received an updated GSR at Issue 3 (ref. [3]).
2. The GSR Tier 1 ‘header’ document explains how the RP will offer the ‘golden thread’ for security based on the design itself, through a risk analysis to the application of a protective security regime. That thread is based on a claims, arguments and evidence framework with a high-level claim that the GSR meets regulatory expectations and one based on SyAPs. These documents also explain the scope for GDA and interaction with other topic areas identifying their relevance to security. The Tier 1 document therefore sets the scene for GDA, explains the scope of their work and outlines their security methodologies, approaches and standards adopted. Issue 3 of the GSR is a more comprehensive document that has drawn on the significant amount of work conducted by the RP in Step 2.

### Secure by Design

1. In developing their security case, and influencing the design itself for security benefit, the RP has adopted an overall ‘philosophy’ of Secure by Design (SbD). In describing that approach, they have included submissions on their SbD methodology, its application and how it informs other topics. The RP’s intent, through this approach to security risk management, is to identify ‘intrinsic’ design solutions and where this is not possible, to adopt ‘extrinsic’ measures to meet regulatory expectations. As SbD is a leading KSyPP, taking this overarching approach to developing a security case is highly relevant and is advancing development of RGP.

### Categorisation for theft

1. Acknowledging a central theme of any security case is the characterisation of the site (design in this case) so to determine the categorisation for theft, the RP produced a methodology. That methodology for assessing the theft risk was demonstrated, albeit in a limited way.

### Categorisation for Sabotage

1. Acknowledging a central theme of any security case is the characterisation of the site (design in this case) so to determine the categorisation for sabotage, the RP produced a methodology acknowledging the UK DBT. Given the maturity of the design, the RP focused on delivering that methodology, based on RGP, to evaluate the design risk from physical attack but also one delivered by cyber means. The RP trialled the methodology against the more mature aspects of the design providing a report on their findings.

### Cyber Security

1. In order to demonstrate how nuclear technology and operations will be protected within the design, the RP developed and demonstrated a methodology for identification and analysis of cyber security risks to CBSIS and Computer-based Security Systems (CBSy). This analysis was informed by their understanding of the threat and application of a SbD approach. The output from this work will inform a conceptual CPS. The CPS will then define the control requirements for an ISS as well as contributing to the identification of vital areas.

### Integrated Security Solution

1. In order to present future licensees with a ‘product’ that supports a licence application and informs a Nuclear Site Security Plan (NSSP), the RP has captured that narrative in the ISS. This element of their security case describes how they will deliver a security protective regime that sits within wider plant risk management. Therefore, the security case is integral to the E3S case and views security mitigation through both the PPS and CPS. Because the development of the ISS will, by necessity, be an iterative approach, and delivered through systems engineering, the details in Step 2 were not fully developed. This was expected and their submission provided a comprehensive framework to be developed in Step 3.

## Basis of assessment: requesting party’s documentation

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

* The GSR, being the security chapter of E3S case (ref. [46]) and (ref. [3]). This ‘header’ document sets the scene for the security case and will eventually capture and summarise the outcome of the GDA;
* Strategy for the Delivery of a GSR for the Rolls Royce SMR (ref. [47]) that provides an early picture of how the full security case will be developed over the GDA;
* Interpretation of the UK DBT for the Generic Rolls-Royce SMR (ref. [48]). Using the UK DBT (ref. [24]), this document provides further context for KSyPP 2;
* Functional Security Categorisation and Classification Methodology (ref. [49]) which outlines the RP’s approach to KSyPP 5;
* Secure by Design Methodology (ref. [50]) which outlines the RP’s approach to KSyPP 1, Secure by Design Analysis (ref. [51]) which outlines the RP’s output from their trials and the Secure by Design Report (ref. [52]) which provides the results of the RP’s ongoing work to influence the design for security benefit;
* Vital Area Identification and Categorisation Methodology (ref. [53]) which outlines the RP’s approach to SyDP 6.2, VAI&C Workshop Output (ref. [54]) which provides evidence of integrated working to inform the risk analysis against sabotage, VAI&C Analysis (ref. [55]) which provides the output from the RP’s trials and the VAI&C report (ref. [56]) which summarises the RP’s work on sabotage;
* Categorisation for Theft Methodology (ref. [57]) which outlines the RP’s approach to SyDP 6.1; Theft of Material & Categorisation Analysis (ref. [58]) which outlines the RP’s output from their trials and Theft of Material and Categorisation Report (ref. [59]) which summarises the RP’s approach to SyDP 6.1;
* Cyber Security Risk Assessment Methodology (CSRAM) which outlines the RP’s approach to SyDP 7.1 and 7.3. This document describes how cyber risk assessment of the design will be conducted (ref. [60]); Cyber Security Risk Analysis (ref. [61]) which provides the analysis from a trial of the CSRAM and Cyber Security Report (ref. [62]) which summarises the cyber security analysis work performed to date in Step 2 and sets out future work; and
* Integrated Security Solution (ref. [63]) which outlines the RP’s approach to FSyPs 6 and 7.

# ONR assessment

## Assessment strategy

1. My strategy was based on the assessment plan (ref. [64]) and informed by the guidance to RPs (ref. [8]) with its specified and implied requirements for both the RP and ONR. My plan explained how my assessment related directly to ONR’s expectations captured in SyAPs and why certain principles are relevant to GDA. In this step, my assessment strategy focus was on the RP’s concept for security - the ‘golden thread’ - and their overall approach to risk management together with methodologies for establishing the magnitude of risk within the design.
2. While not the primary focus, I wanted to see how the RP’s risk analysis and wider security thinking shaped the selection and design of the physical and cyber security protection systems. Detailed design of protective systems, underpinned by credible risk analysis, is expected in Step 3. However, in Step 2 it is necessary to set the conditions for more detailed work on their security design. The KSyPPs figured prominently in my assessment as these principles inform any security case. Therefore, my expectation was that the RP had considered SbD, the threat, graded approach, defence in depth, functional categorisation and classification and codes and standards that would inform the security solution. Furthermore, that consideration was given to how their analysis would shape a future security case after GDA that would likely meet regulatory and legal expectations. I therefore wanted to see the RP’s framework for a security case that would be developed further in Step 3.
3. While not an assessment topic as such, my strategy included close coordination with C&I. The interaction between C&I and cyber security has been prominent in my assessment strategy.

## Assessment

### Generic Security Report

1. Step 2 is the first substantive technical assessment step. The focus of my assessment in this step was towards the fundamental adequacy of the RP’s security case captured through a tiered approach and based on claims, arguments and evidence. At Tier 1 is the GSR - a ‘header’ document - that is both a scene-setter and summary of work carried out at subsequent tiers. The RP presented their GSR at Issues 1 and 3 (ref. [46] and ref. [3]) that represents a high-level picture of their case.
2. I assessed the RP’s GSR header document at the beginning of the step although it was not yet informed by lower-level Tier 2 and 3 documents. This was anticipated, and I was not expecting a fully developed submission as this would be unrealistic. Also, my assessment effort would, in this step, be towards the adequacy of their risk methodologies and how they would inform the protection schemes in sufficient detail to be of use to a future licensee. I also assessed the RP’s arrangements for developing the GSR into a security plan for licencing. My assessment was informed by the guidance to RPs (ref. [8]) and the GDA Security TAG (ref. [16]) that draws from previous GDA assessment experience. I looked specifically for alignment with the relevant SyAPs and expected the RP to draw from the KSyPPs given their relevance to a header document.
3. Notwithstanding this was the first iteration of the GSR (in Step 1 I received a Preliminary Security Report), I concluded that there was an opportunity, albeit early in this step, for this header document to be more than a framework and include an expanded structure outlining their security ‘philosophy’. My expectation was that SbD would feature significantly in this report as this approach offers opportunities to reduce risk given the immaturity of the design. Essentially, how risks would be considered, managed, systems modified (or areas embellished) to reduce risks and any deconfliction with other requirements (explaining how this is achieved). While the submission did not fully exploit this opportunity, it does provide a suitable framework for the next version. Also, it is meaningful when considered alongside the Strategy for Developing the GSR (ref. [47]). I found this to be the case because the strategy document covers a significant number of relevant topics including how the GSR fits in with the E3S case.
4. The second issue of the GSR (ref. [3]), however, provides a significantly better scene setter and summary drawing on several strands of work in this step. This more developed submission captures all the expected security topics and leads the reader in a logical manner from how the security case sits within the wider E3S case through to how it will be developed further, after GDA, to meet regulatory expectations. The document explains how the RP is working within their engineering processes, has embraced SbD and developed their risk analysis so to inform a security regime.
5. Therefore, for this header document, and at Issue 3, I conclude that the information submitted is consistent with RGP and provides a suitable framework to develop the case in Step 3. I confirm that the design reference (ref. [65]) is consistent with the design I have assessed during Step 2

### Secure by Design

1. SbD is a KSyPP within SyAPs. The application of which ensures the integration and influence of security alongside nuclear safety as the design matures. In addition to enabling deconfliction, this approach provides a means by which security risks might be designed-out or mitigated early in the design so to meet security outcomes, achieve efficiency and cost effectiveness (ref. [23]).
2. The security design is being developed as the RP progresses through GDA. Understanding the benefits of adopting a SbD approach, the RP has made it a fundamental principle within their security philosophy. I assessed the RP’s SbD approach as described within the following submissions:

* SbD Methodology (ref. [50]).
* SbD Analysis (ref. [51]).
* SbD Report (ref. [52]).

1. As a KSyPP, SbD is relevant to several FSyPs within SyAPs (ref. [5]). Therefore, I targeted additional submissions to assess the practical application of SbD so to inform my overall judgement. These include the following:

* Categorisation for Theft Analysis (ref. [58]) and Report (ref. [59]).
* VAI&C Methodology (ref. [53]), Analysis (ref. [55]) and Report (ref. [56]).
* Functional Security Categorisation and Classification Methodology (ref. [49]).
* Cyber Security Risk Assessment Methodology (CSRAM) (ref. [60]), Analysis (ref. [61]) and Report (ref. [62]).

#### Secure by Design methodology

1. It was my expectation for Step 2 that the RP demonstrate an understanding of SbD, as reflected within RGP (see Section 2); and develop an appropriate and adequate methodology with which to integrate the security team within the wider design and engineering activities. I further expected that the methodology demonstrates adequate processes with which to influence the design as it matures and remove or mitigate security vulnerabilities through deconfliction at the earliest opportunity. Whilst the opportunities to demonstrate the latter may be limited due to the immaturity of the design at this stage of GDA, the setting out of principles, processes and practices, would set the foundation for activities within Step 3 where ONR’s expectations will be expanded as part of our ongoing assessment.
2. The SbD Methodology (ref. [50]) describes a nine-step process defining the relevant principles and objectives; the triage process to identify security relevance and involvement; the identification of vulnerabilities and safety-related hazards; the describing of initiating events of malicious origin (IEMO); to inform Defence in Depth (DiD), security requirements and the subsequent categorisation and classification of security systems.
3. It is my opinion that the RP has demonstrated an innovative approach, as it seeks to align its application of SbD with its engineering processes. Whilst I identified that this ambition has, on occasions, introduced a degree of complexity, I also recognise that the RP is building upon mature and long-standing engineering-based processes to facilitate company-wide integration. There is an occasional lack of clarity within the methodology which is, in part, a symptom of the RP’s efforts to apply SbD to an established engineering process, rather than build its engineering processes around the SbD principle. However, I assessed that this is not to the overall detriment of the approach taken, and I support the RP’s innovation in this regard. It is my assessment that the methodology includes all the relevant aspects for consideration, and in principle, provides an adequate framework for an integrated process.
4. Demonstrating the practical application of the SbD approach, the RP presented evidence of SbD being informed and applied through ‘Phase 0’ of its VAI&C methodology (ref. [53]). This is intended to provide early, security-informed input into the design process by building upon a number of assumptions and judgements prior to a formal application of the methodology. In doing so, this represents one of the feedback loops described within the nine steps of the SbD Methodology (ref. [50]) to continually review opportunities to reduce vulnerabilities as the design matures. Phase 0 is an early application of the SbD principle at a time when the ability to influence design is arguably at its greatest. Subsequent assessment of the RP’s VAI&C analysis (ref. [55]) goes on to demonstrate some early examples to reduce risk from sabotage having applied the VAI&C methodology.
5. It is my judgement that the RP has demonstrated a mature understanding of SbD which reflects the RP’s longstanding engagement on the subject including its involvement in the government funded research on SbD in 2020 (ref. [66]). The RP’s submission of a partial trial of its methodology is judged to be a positive initiative reflecting the RP’s ambition. Whilst I recognised the RP’s limited opportunity at this stage to demonstrate its security integration and influence upon the maturing safety-centric design, these would form part of my Step 3 focus.
6. I raised a multifaceted RQ (RQ-01025, ref. [67]) which sought clarity on integration across purposes and was closed following the RP‘s response. The response provided me with sufficient assurances, and I agreed that any relevant changes could be captured in future iterations of the document and the subsequent analysis (ref. [51]) and report (ref. [52]) submissions.
7. I judge that the SbD methodology (ref. [50]) meets expectations for Step 2 in that the methodology is fundamentally adequate. It demonstrates a satisfactory understanding of SbD and its principles, and includes the appreciation of early engagement across design topics.
8. During Step 2, the RP demonstrated its progression of the SbD methodology through the submission of SbD analysis and report documents. I assess that these further demonstrate the RP’s ambition and reflect its recognition of SbD as fundamental to the formative phase of design development.

#### Secure by Design analysis

1. The RP subsequently carried out an assessment of its application of the SbD methodology. It has done so by applying aspects of the methodology against chosen systems which are described in its SbD analysis submission (ref. [51]). I consider this to be a positive endeavour towards ensuring the methodology is fit for purpose and achieves its objectives. It also provides the RP with an opportunity to refine the methodology based upon practical lessons learnt. Furthermore, whilst I judge that the SbD methodology is not unclear, this process delivers additional clarity, adding value to what could be viewed as a complex process.
2. This SbD analysis, in applying the SbD Methodology, is restricted by the current design immaturity. However, I assess that this does not detract significantly from its objectives, providing a useful exercise in demonstrating aspects of the process and identifying areas for improvement.
3. The SbD analysis applies the SbD methodology to two areas of the plant, the Spent Fuel Storage & Cask Loading System (FAB) and the reactor Diverse Protection System (DPS). I assess that these represent an adequate degree of diversity with which to test the methodology’s broader application, and furthermore, demonstrate an examination of wider cross-purpose interaction with the latter having cyber security and C&I relevance. I judge the analysis is forthcoming in identifying areas for improvement which demonstrates transparency and attention to detail, as well as the pursuit of continuous improvement. I take confidence from this but will continue to track the recommendations being made and follow-up in Step 3 on the anecdotal resolution plans being laid out at this stage to ensure the veracity of intent and security influence. Furthermore, I will continue to assess the RP security team’s influence as broader Structures, Systems and Components (SSCs) develop throughout the design. I reiterated that despite the SbD methodology’s adequacy at this stage of GDA, without meaningful influence on the design facilitated by strategic documentation, well-defined processes and cultural buy-in from the organisation as a whole, the application and the potential for SbD to make the desired impact will be limited. Despite the confidence I have through engagement thus far, I raised an RQ.
4. I raised an RQ (RQ-01204, ref. [67]) against the SbD analysis focused upon gaining further confidence on the strategic application of SbD through documentation and consultation.
5. The RP makes reference to security modifications affecting construction materials and the nature of energetic chemicals which requires appropriate deconfliction. Further to this, I also sought clarity on the RP’s plans for the design-wide application of the SbD methodology and the necessary manageability.
6. The RP stated that their practical applications were more mature than their written submissions. However, they had planned to produce additional documentation including a written Standard to promote the visibility of the SbD principle across their purposes. These will develop alongside the Technical Report Group meeting, where cross-purpose interactions are discussed. This provides me with confidence that high-level representation of SbD is progressing alongside expectations. However, I did suggest that the development of an appropriate ‘integration strategy’ may have merits. Whilst there exists a C&I and Cyber Security Integration Strategy (ref. [68]), which is subject to ONR C&I assessment, a holistic security integration strategy is lacking.
7. The RP acknowledged that lower-level processes and procedures were currently absent but would be developed. It is my judgment that this has the potential, if not addressed in a timely manner to result in a suboptimal application of SbD. Positively, the RP was able to point towards some useful work whereby assessment into the application of the SbD principle is being carried out systematically using a ‘SbD Database’ against various parts of the design by the security team.
8. I assess this to be key evidence towards implementing a holistic application of SbD. I judge this to be beneficial in identifying resource requirements, identifying gaps, and assessing the level of consultation to ensure security input into the design phase across the facility. Although this work is yet to be formally submitted to ONR, it provides me with confidence that the RP intends to apply the SbD Methodology completely and holistically.
9. The RP responded to the RQ in full (ref. [67]). I considered this to be a satisfactory response to areas where I sought clarity and reassurance. Some aspects have been recorded by the RP and noted for consideration within Step 3 as the design matures. This reflects the overall adequacy of the RP’s SbD methodology to date.

#### Secure by Design report

1. The RP submitted their SbD Report (ref. [52]) for assessment. Aside from providing additional clarity through a summary of the work carried out to date, I judge this to adequately reflect the RQs (ref. [67]) previously raised and provides a written reflection of the discussions held. Significantly, this includes written commitment to produce and apply the aforementioned ‘Security Requirements and Analysis Standard’ to support guidance and governance purposes; as well as the ‘SbD Database’ serving as a statement of technical accounts and assessing traceability of the SbD workstreams.
2. In addition to meeting expectations for Step 2 GDA, the SbD report clearly identifies the direction of travel and provides assurances that the SbD methodology will continue to be refined. Whilst it is too early to judge whether SbD will be adequately applied to influence the design optimally, as a multitude of facilities mature, I assess that the foundations for achieving success are adequately demonstrated at this stage.

#### Key risk assessment methodologies

1. The ONR security team have identified key risk assessment methodologies for detailed assessment in their own merit. These methodologies, including VAI&C and Cyber Security Risk Assessment Methodology (CSRAM), are key in taking a risk-based approach towards meeting security outcomes in alignment with SyAPs. Furthermore, both are fundamental processes towards eliminating or mitigating risks early in the design phase, and are integral to an SbD approach. The SbD methodology section makes reference to ‘Phase 0’ in respect of the VAI&C work (See section 4.2.2.1), but the RP’s CSRAM (ref. [60]) has also been assessed.
2. The CSRAM, while separate from the core SbD methodology, also incorporates elements of a SbD philosophy through its use of the IEC 62443-3-2 standard (ref. [34]). This allows for an iterative multi-step approach to assessing and mitigating cyber risks, and a process of partitioning systems into security zones and conduits based on their security and safety significance. These zones can then potentially be modified based on further CSRAM assessments or the application of the SbD methodology itself to allow a system architecture informed by security risk and the graded approach.
3. I therefore judge that the RP’s approach to SbD has not been developed in isolation and is adequately referred out to in other aspects of my Step 2 assessment.

#### Wider applicability of Secure by Design

1. I have further assessed the overarching nature and application of SbD through the examination of additional RP submissions. In addition to the risk assessment methodologies discussed above, I assessed the RP’s Functional Security Categorisation and Classification (ref. [49]), and Theft of Material and Categorisation (ref. [58]) submissions. I judge that these submissions demonstrate both the RP’s understanding of the interconnectivity between these processes, and in applying them appropriately given the strategic importance of SbD. These submissions meet my expectations which are reflected within the relevant TAGs (ref. [6]) in which security functions and SSCs are categorised and classified in accordance with their significance for security; and that categorisation for theft is applied in line with RGP and on a site-wide basis.
2. Furthermore, the RP’s comprehension of SyAPs as a sequential process towards achieving an adequate security posture can be inferred from this breadth of assessment. This further includes my assessment of the RP’s Threat Interpretation submission (ref. [48]). ‘The Threat’ is another of ONR’s KSyPPs (ref. [5]) which is fundamental towards meeting security expectations. It is my expectation that this be applied and utilised across the risk assessment methodologies, and that these, and the eventual plant security protective systems, be designed, evaluated and tested using the UK DBT.
3. The RP’s ability to utilise the UK DBT (ref. [24]) was initially delayed following access and handling challenges of this sensitive document. This resulted in the early application of a surrogate DBT to progress with and demonstrate the early phases of their risk assessment processes for VAI&C. Whilst the RP was able to make some assumptions around the threat, and its application pertaining to the various methodologies, the opportunities to apply the UK DBT in full, and against the full spectrum of risk has been limited.
4. The RP’s stated intention to apply the UK DBT in full in Step 3 provides me with a degree of assurance that an adequate foundation for security assumptions is in place in support of key risk assessment processes. However, use of a surrogate, rather than the UK DBT introduces a degree of project risk at this stage. That said, the RP continues to demonstrate an innovative approach, applying methodologies derived from, and suited to cyber security, namely a serialisation scheme used to express threat information and the relationships between them (Structured Threat Information Expression (STIX)). I judge the RP’s approach to assessing cyber threats drew on an appropriate range of government, industry and sector specific threat information and demonstrated good alignment with the articulation of cyber threats in the current UK DBT.
5. I raised an RQ (RQ-01067, ref. [67]) whereby an adequate response has been provided to a number of points seeking clarity. However, as the RP looks to develop its processes involving a nuanced application of the UK DBT, the assessment of the UK DBT’s application to inform numerous processes and methodologies will be revisited in Step 3. The RP’s security team is cognisant of the importance of communicating the threat, as appropriate, with designers and engineers in the interests of applying SbD.
6. I assess that the RP has met my expectations in terms of understanding ONR’s KSyPP 2 (ref. [5]) as fundamental towards mitigated risk both as part of SbD, and in defining an adequate security design later in Step 3. I have delivered my Step 3 expectations to the RP with regard to SbD. Whilst it is my judgement that the RP has met expectations for Step 2, I expect to see increased evidence of practical integration of security across its specialisms to influence the maturing design. Whilst a statement of intent, in the form of strategic documentation and some evidence of engagement has been provided, it is essential that the RP maintains this impetus ahead of the potential for inherent risk reduction being reduced or lost.

#### Section conclusion

1. In summary, the RP is focused on applying the SbD principle towards reducing and mitigating risks as their design matures. SbD is an overarching principle, key to a number of security-related principles as described within SyAPs, and is fundamental to a number of risk assessment methodologies. As such, I have focused on three SbD submissions including a wider body of related submissions with which to form my judgement. I recognise that RGP on SbD is limited. However, the RP’s SbD methodology (ref. [50]) aligns with the RGP available, including ONR’s corresponding TAG (ref. [23]), and is judged an adequate fundamental methodology to meet Step 2 expectations. Furthermore, I assess that through the SbD analysis (ref. [51]) and SbD report (ref. [52]), the RP has sought to refine the methodology and demonstrate a commitment towards ongoing improvement and site-wide application that is key to meeting expectations within Step 3. The RP has met my expectations.

### Categorisation for Sabotage

#### Introduction to Vital Area Identification and Categorisation

1. VAI&C is the process of identifying the areas at a nuclear facility around which protective security measures should be provided to reduce the risk to the public from an Unacceptable Radiological Consequence (URC) arising from sabotage.
2. The VAI&C concept is used to define a boundary around vital SSCs, Nuclear Material (NM) or Other Radioactive Material (ORM) and categorise these areas in accordance with Security Delivery Principle (SyDP) 6.2 and Table 1 in Annex B of SyAPs (ref. [69]). This categorisation directly informs the PPS outcome and indicative security posture in accordance with SyDP 6.3 and Annex C of the SyAPs, which in turn dictates the required response strategy as set out in SyAPs Annex D.
3. If vital areas are not properly identified then it is likely that insufficient, ineffective or inappropriate PPS and protective security arrangements will be implemented in attempts to mitigate public risk. For GDA, early and accurate identification of vital areas supports the SbD principle and allows for changes to be identified to the reactor design to minimise the opportunities for, and consequence from, sabotage once the reactor is operational. As the design matures, or aspects of it are frozen, the benefit that could have been realised from adopting the SbD principle diminishes.

#### Assessment introduction

1. The focus of the VAI&C assessment topic is reflected in the broader Step 2 assessment plan (ref. [64]). Essentially, for VAI&C, this sets the expectation for two key objectives to be met. Objective one is for the RP to develop a set of written arrangements, in a methodology document, for the identification of vital areas in accordance with RGP. This is to ensure that the security risks to the reactor design can be identified in sufficient detail, commensurate to the design maturity, through the adoption of a standardised process which is capable of producing consistent outputs when reapplied.
2. Objective two was for the RP to demonstrate the application of its VAI&C arrangements through a trial study to identify security risk to a discreet set of high consequence and significance SSCs, which are relatively mature in design. This is intended to demonstrate the ability of the arrangements to accurately identify security risks and to show that they are capable of producing consistent outputs when applied to the wider design as it matures in Step 3.

#### Vital Area Identification and Categorisation methodology

1. The RP’s VAI&C methodology document can be found at (ref. [53]). At a high level the methodology consists of a process broken down into five distinct phases, 0 to 4, which are described below along with my judgments as to the extent to which each phase aligns with RGP. This RGP is predominantly ONR TAG 6.2 (ref. [20]), IAEA NSS 4 (ref. [28]) and IAEA NSS 16 (ref. [26]), unless otherwise stated.
2. Phase 0. The Rolls-Royce Small Modular Reactor is a new reactor design with no reference plant. As such, design assumptions based on engineering judgement should be made early in the design process in order to provide timely security-informed input to indicate the likely location of the vital areas. This approach supports early application of the SbD principle at a time when the ability to influence the design is arguably at its greatest. I further consider this approach to be aligned with IAEA guidance which states that the VAI&C process should be applied as early in the design phase of a new facility as possible when physical protection might be optimised and retrofitting avoided (ref. [26]). The process steps described in the RP’s methodology for Phase 0 meet my expectations.
3. Phase 1. In this phase the RP collates relevant information, establish an assessment team, create links with other technical disciplines and determine gaps in information. A more detailed description of this phase is provided in section 4 of the RP’s methodology (ref. [53]). I judge that the intent of this phase, as described, aligns with both my expectations for the preliminary activities required to conduct thorough VAI&C analysis in line with RGP. Specifically, fundamental aspects of IAEA guidance described in Section 2 of NSS 16.
4. Phase 2a. This phase, described in detail in section 5.2 of the RP’s methodology, aims to quantify future NM/ORM holdings and apply a highly conservative screening process to determine the potential to generate an URC. The conservative nature of this phase should apply an unmitigated release assuming 100% dispersal. The intent is to identify the NM/ORM with URC potential which may require protection from sabotage, but more importantly identify the NM/ORM without URC potential so that it can be excluded from further analysis. The methodology claims that this analysis will consider the bounding inventory at each specific plant location during any point in the SMR lifecycle. I consider this approach to align with standard practice for VAI&C and it reflects IAEA guidance described in section 2.2.3 of NSS 16.
5. Phase 2b. This phase considers the inventory with URC potential identified in Phase 2a and follows a structured process to determine the potential means by which that URC might be caused. It includes both direct sabotage of the NM/ORM itself and malicious acts, or combinations of, which could cause the loss of the Fundamental Safety Functions (FSF) which keep the NM/ORM in a safe state. The SSCs needed to be sabotaged to induce a loss of FSF and cause the URC are identified as potential targets and their locations identified and documented. Combinations of sabotage-related failures, termed Potential Sabotage Event Scenarios (PSESs), are also derived at this stage to inform subsequent phases of the analysis. The above process is described in greater detail within section 5.3 of the methodology. My assessment of this phase of the methodology was carried out against IAEA NSS 16. Although my assessment identified minor differences in approach against sources of RGP these were discussed with the RP. The RP provided assurances that the overall outcome would meet the intent of the VAI&C process, to identify security risks to the design. As a goal setting regulator, divergence from process, set out RGP, presented me with little concern at this stage of GDA given the RP’s assurances that ultimately the overall VAI&C objectives would be met. An example of a differing approach between the RP’s methodology and RGP is provided in the paragraph below.
6. RGP describes the use of sabotage logic models which provide a structured approach and effective means of adopting and adapting the safety case analysis to identify Initiating Events of Malicious Origin (IEMO) and PSES. The RP’s methodology did not appear to adopt such an approach and instead placed greater reliance on workshops attended by Subject Matter Experts (SME) to identify the IEMOs using what appeared to be a less structured process. My intention was to determine the adequacy of this divergent approach through the RP’s demonstration of the application of the methodology later in Step 2. My assessment considers this in greater detail below.
7. Phase 3a. This phase applies the UK DBT to the output of the high-level Phase 2b assessment to confirm, or otherwise, if the combinations of events identified in Phase 2b are credible for an attack group to achieve success. Credible combinations are termed as Sabotage Event Scenarios (SESs) and the targets within them are identified as potential sabotage targets. The SESs are taken forward for radiological consequence assessment in the next phase. A detailed description of Phase 3a is set out in section 6.2 of the RP’s methodology document. From my assessment of the detail presented, I conclude that this section of the methodology broadly meets my expectations for how a DBT should be applied to the VAI&C process. It is also in broad alignment with Section 2.6 of IAEA guidance (ref. [26]).
8. However, the success of Phase 3a of the RP’s process is dependent on an accurate set of hazards being applied to the analysis in order to determine what is, or is not, credible for the attack force to achieve. These hazards in the UK context are defined in the UK DBT. Although the RP’s methodology states that the threat interpretation for the RR SMR programme will be based upon the UK DBT. During an early L4 engagement the RP stated its intention to use an alternative DBT to inform early iterations of its VAI&C analysis. It explained that this was to reduce the security classification of those early analysis reports. I advised the RP that this was an area of concern and explained that as the UK DBT sets out the hazards against which the security risks are derived, using a dissimilar set of hazards is likely to invalidate its VAI&C analysis application to the UK. The RP stated that, whilst use of an alternative still facilitates proof of concept of its methodology, it was a temporary measure whist controls were being put in place to provide its SMEs with access to the classified UK specific document. It provided assurances that the UK DBT would be used in the latter stages of Step 2. I was satisfied with this response at the time, given that it was early in the step, and reserved judgement until later in the step. Further details of end of step judgement can be found below.
9. Phase 3b. This phase is intended to determine the final damage state of the plant once subjected to the UK DBT and goes on to determine the resultant radiological consequences for each sabotage end state. Areas that contain targets which, if sabotaged either alone or in combination with other sabotage events, could lead to an URC are categorised as vital areas applying the graded approach in accordance with Table 1 of Annex B of SyAPs. I judge this phase of the process, as described in detail in section 6.3 of the RP’s methodology and when compared to RGP, to meet my expectations. However, my overall judgement as to the adequacy of this phase was to be informed by the demonstration of application of the RP’s methodology which is covered in greater detail below.
10. Phase 4. This phase takes the tabular output from Phase 3b which defines the location and categorisation of vital areas and, using available layout/floor plan information for relevant buildings across the site, plots them on the floor plans to provide a visual representation of the design’s vital areas. I consider this means of presenting the vital area location data to be a valuable representation to aid in planning and evaluating the consequences of the threat for future VAI&C reviews and to assist in PPS evaluation.

#### Section conclusion

1. Overall, I consider the content of the RP’s VAI&C methodology submission to broadly meet with my expectations and be in alignment with VAI&C RGP as a standalone process. However, overall judgement of adequacy is made through my assessment of the output from its application through the trial study. I therefore consider the first objective of my VAI&C Step 2 assessment strategy, to develop a VAI&C methodology in accordance with RGP, to have been met.

#### Vital Area Identification and Categorisation analysis

1. The second part of my VAI&C assessment covers objective two of Step 2, the RP’s demonstration of application of its arrangements through a trial study. As part of this process, the RP produced the following documents which are developing iterations of the final submission. This has been the primary focus of this part of my assessment;

* Rolls-Royce SMR: Vital Area Identification and Categorisation Analysis, SMR0008452 Issue 1 (ref. [55]).
* Rolls-Royce SMR: Vital Area Identification and Categorisation Report, SMR0009689 Issue 1 (ref. [56]).
* Rolls-Royce SMR: Vital Area Identification and Categorisation Analysis, SMR0008452 Issue 2 (ref. [70]).

1. In order to meet the agreed VAI&C objectives for Step 2 of this GDA I would expect the following to be met in accordance with RGP. Through the application of the DBT relevant to the UK, a demonstration that the proposed VAI&C methodology is capable of accurately determining the effects of, and consequence from, sabotage acts delivered by the full range of threat vectors set out in RGP. The focus for demonstration purposes in Step 2 should be on a selected set of high reliability SSCs that provide fundamental safety functions and allow for the full scope of the VAI&C methodology to be exercised. The range of threat vectors to be considered are from physical and kinetic energy threats alone and in combination with cyber threats. The combination threats are described as ‘blended attacks’ in RGP. Cyber attacks conducted in isolation should also be considered. When considering physical attack, analysis of a range of delivery methods must be demonstrated including:

* Direct attack which involves the energetic materials described in the UK DBT being deployed in contact with, or in close proximity to, the NM/ORM in order to disperse it. Or a deliberately generated criticality event;
* Indirect attack which does not involve direct targeting of NM/ORM but involves compromising the functionality of safety critical SSCs the failure of which could initiate fault sequences leading to an URC. This compromise could be through the physical disablement of SSCs using either energetic materials or manual adversary actions, and;
* Consideration must be given to both Type 1 attacks which are those deployed from within the site or facility boundary and Type 2 attacks which are those deployed from off site.

1. The RP’s chosen set of SSCs against which to perform its trial study and identify security risk was what it termed the Fuelling Block which consists of the Spent Fuel Pool (SFP), cask pit, new fuel storage and inspection area and fuel transfer routes. These SSCs were selected on the basis that their design was comparatively well developed at the time of the trial.
2. The trial itself was conducted through two VAI&C workshops. The first workshop was in support of Phases 1 and 2 of the VAI&C methodology and is recorded in the workshop output (ref. [54]). The second workshop was held in support of Phase 3a. Its output is documented in the VAI&C report (ref. [70]) and its supporting references.
3. My assessment of the RP’s trial VAI&C study is detailed in the following section of this report. It considers each of the five phases of the methodology, as described above, along with my judgments against RGP. This RGP is predominantly ONR TAG 6.2 (ref. [20]), IAEA NSS 4 (ref. [28]) and IAEA NSS 16 (ref. [26]), unless otherwise stated.
4. Phase 0. I have not considered this phase in significant detail as part of my assessment as its intent is to inform and support the RP’s SbD philosophy which is covered in greater detail in section 4.2.2.1 of this report. However, I did sample some of the claims relating to phase 0 to assure myself that the RP was providing an appropriate level of focus to the SbD process from a VAI&C perspective, i.e., to design out vital areas. I requested for my assessment an optioneering decision record for the reactor island pools structural form (ref. [71]). In short, from my assessment of this submission, I am satisfied that it provides evidence to demonstrate that a formal engineering optioneering process had been adopted by the RP to determine the strengths and limitations of a range of materials for the construction of the reactor pools. Security SQEP was represented on the optioneering panel with their input leading, in part, to the selection of construction materials with good resistance to the effects from explosive ordnance for a Class 1 SSC delivering a security function. I expect to see further examples to demonstrate that attempts are being made by the RP to either limit the number of vital areas or fortify them through security design improvements early in Step 3.
5. Phase 1. The first phase of the RP’s VAI&C process is preparatory and involves gathering relevant information and convening a panel of experts to support the VAI&C process. My assessment of the specialists selected showed knowledgeable representation in the areas of radiological consequences and inventory, plant design, operations and layout, safety case and security. I observed one important and notable exclusion from the panel of experts being representation from cyber security which is critical for VAI&C to ensure the accurate identification of URC pathways through blended attack vectors. I raised this as an observation at a routine L4 engagement, the RP stated that this was an unintended omission and that this learning would be carried forward to ensure there is sufficient cyber security representation at all future Step 3 workshops. This will be a specific area of regulatory focus in Step 3 to ensure cyber security is sufficiently integrated into the VAI&C processes.
6. During this phase the RP also gathered the available inventory data to inform later phases of its analysis. The submission shows that gaps in data were identified but informed engineering judgements, or assumptions, were made as to likely future inventory holdings. This information is detailed in Table 10 of Appendix A of the submission (ref. [55]) which I judge to demonstrate that a forward looking assumption based approach has been adopted. Further commitment is then made to formally review the VAI&C analysis as inventory data is refined later in GDA. I consider this to be a pragmatic approach and one which provides a sufficient level of detail to enable the RP to adequately conduct a trial of its methodology.
7. In addition, the identification of modes of NPP operation during different parts of the plant’s lifecycle is a key requirement for VAI&C analysis as set out in IAEA NSS 16. The RP’s submission reflects this and states that each mode will be subject to evaluation within this GDA.
8. This meets with my expectations and sets clear boundaries for the Step 3 VAI&C analysis. For the purposes of the trial study in Step 2, the RP has presented detail covering various modes of operation when the pools contain spent fuel. I judge that this should provide sufficient scope for the complete demonstration of its methodology.
9. Phase 2a. The purpose of this phase is for scoping calculations to be carried out to conservatively determine which of the assumed inventories from Phase 1 have URC potential and which can be screened out from further analysis. Adopting this type of screening approach aligns with RGP (ref. [26]) which states that ‘conservative analysis should be performed to determine the potential radiological consequences of the complete release of each nuclear or other radioactive material inventory. The analysis should be performed without consideration of mitigation measures present at the facility. If the potential radiological consequences under these conservative analysis conditions are below the URC threshold, sabotage leading to an URC is not possible’.
10. However, my assessment identified the use of detailed radiological consequence analysis being carried out in this phase which is intended for use in Phase 3b. This included dose reduction factors being applied to the RP’s unmitigated screening calculations. Coupled to this there also appears to be the potential for double accounting of those reduction factors. Noting that this level of analysis should only be applied during Phase 3b, but is included in this phase of the RP’s trial, the following paragraphs detail my assessment observations against its use.
11. Firstly, in terms of double accounting, the RP’s methodology presents an equation for determining the quantity of material released in a respirable form from a DBT event. This includes a damage ratio to account for the fraction of the inventory dispersed by the DBT and an Airborne Release Fraction (ARF) to represent the fraction of material which is suspended in the air from the event. These two input parameters appear to be the same and so care must be taken in their application to avoid an over-reduction or miscalculation of dose consequence. Although there is no evidence of double accounting at this stage, the equations appear to lend themselves to the potential for error, focus will therefore be placed on these calculations during my Step 3 assessment.
12. The RP’s analysis applies dose reduction factors at this phase in the process which is intended to be for screening purposes only. In its Phase 2a calculations it has applied a Decontamination Factor (DF) of 10 for partial retention of the release by the building structure and in some cases a Respirable Fraction (RF) of 0.1. This accounts for an overall reduction factor of 100 meaning that the screening calculations which are supposed to be unmitigated are only taking account for 1% of the potential inventory as opposed to the intended 100%. This approach is not in alignment with RGP or the RP’s Phase 2a methodology which states that a conservative approach will be applied whereby the worst-case conceivable sabotage related release will be considered. In accordance with the RP’s own arrangements this level of detailed analysis should only be introduced during Phase 3b.
13. The analysis goes on to model the release of dispersed material from within the fuelling block containment structure which again represents detailed VAI&C radiological consequence analysis, not conducive to a conservative screening approach. The submission describes the application of building wake effects and claims that air turbulence from wind flowing past the building will influence the distribution of released material and that released activity can be assumed to be instantaneously dispersed throughout the wake volume. This is a strong claim, one which I will expect the RP to fully substantiate with evidence during Step 3 of GDA, particularly for high energy UK DBT dispersal events. The building wake model is typically used in safety analysis for low energy unpressurised releases. Therefore, prior to application of this approach the RP will be required to demonstrate that it is validated to accurately model high energy, high pressure, explosively driven events. This demonstration is required in accordance with the following ONR Safety Assessment Principles;

* ONR SAP AV.1 – Assurance of validity of data and models, Theoretical models. This states that theoretical models should adequately represent the facility and site. It is important that the post DBT attack damage status of the facility is taken into account.
* ONR SAP AV.2 – Assurance of validity of data and models, Calculation methods. This states that calculation methods used for analyses should adequately represent the physical and chemical processes taking place.
* ONR SAP AV.3 – Assurance of validity of data and models, Use of data. This states that data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.
* ONR SAP AV.5 – Assurance of validity of data and models, Documentation. This states that documentation should be provided to facilitate review of the adequacy of the analytical models and data.
* ONR SAP AV.6 – Assurance of validity of data and models, Sensitivity analysis. This states that studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.

1. A further observation is the use of a modelling tool called HOTSPOT which, although not used in the Step 2 analysis, is cited as being an appropriate model in other RP VAI&C submissions. It should be noted that the developer of this model has only verified its use for accident analysis in open air conditions where no building containment exists which restricts the dispersal of material to atmosphere. Should the RP choose to apply this model in Step 3 prior justification must be provided with respect to the conditions in which it is applied and in accordance with ONR SAP AV.1, AV.2, AV.3, AV.5 and AV.6.
2. My assessment of the RP’s selected modelling tools has been informed by ONR Technical Assessment guide NS-TAST-GD-045 Radiological consequence analysis for fault conditions (ref. [21]). Additionally, advice has been provided on this topic area from an ONR Radiological Consequence Analysis specialist inspector. This advice states that due to the degree of uncertainty in VAI&C analysis, and in the absence of verified codes to model explosively induced releases within containment structures, a standard R-91 gaussian plume model should be applied to ensure levels of conservatism are maintained. This will remain my expectation throughout GDA until such time that the RP provides evidence to satisfy the above ONR SAP AV series for each of its selected dose consequence models.
3. A separate observation is that some of the parameters cited in the RP’s equations, such as the DR and DF, can only be determined through application of the DBT. During Phase 2a of the RP’s process the DBT is yet to be applied and so further clarification will be sought as to why the RP has introduced its detailed VAI&C analysis prematurely which is not in alignment with its own methodology and risks the miscalculation of dose consequence later in the process.
4. A positive observation is that analysis covering a maliciously generated criticality event within the reactor pools building is included within the submission. I judge this to be an encouraging demonstration of the extent to which the RP is considering different attack vectors.
5. The trial analysis report was submitted at the end of Step 2 at a point when this AR was being drafted so although not raised at the time of writing it is my intention to raise a Step 2 RQ around the RP’s use of reduction factors in its screening analysis. My assessment of the RP’s response will be covered in the ONR Step 3 assessment report. Furthermore, particular attention will be provided as to the applicability of the RP’s selected dose consequence models for DBT induced events in Step 3.
6. Despite my assessment of this phase identifying a number of areas requiring follow-up action, overall I am satisfied with the output of this phase in as much as the overall conclusion is that spent fuel has URC potential. This meets my expectations.
7. Phase 2b. For each inventory type with URC potential identified in Phase 2a, the RP uses this phase to analyse the design, predominantly using the safety case data, to determine which SSCs would need to be challenged in order for an URC to occur. This is based around consideration of each FSF which ordinarily ensure that the NM/ORM is maintained in a safe state. The high level FSFs are control of reactivity, cooling/heat removal and containment of radioactive material. It is expected that this analysis be carried out for each plant operating state in Step 3.
8. Malicious actions, aligned to the UK DBT, which could compromise SSC performance and hence FSFs are termed Initiating Events of Malicious Origin (IEMO) and combinations of sabotage events required to generate an URC are termed Potential Sabotage Event Scenarios (PSES). It is often the case that IEMO and PSES are analogous to Postulated Initiating Events (PIE) (accidental events or failure conditions) which are identified through the safety case analysis in both the Probabilistic Safety Analysis (PSA) and the Fault Schedule (FS). The safety case data therefore acts as an initial building block for the VAI&C analysis for NPPs. The RP acknowledges this in its submission, however it confirms that at this stage in GDA there is insufficient design information available, and hence a mature safety case, to be able to develop detailed IEMOs and PSES from the PIE. ONR fault studies inspectors confirmed this to be the case at the time of writing.
9. Additional IEMOs and PSES which would have been excluded from the PSA and FS based on a low frequency of occurrence must also be reintroduced to the VAI&C analysis due to them remaining credible security case targets given the probability assigned to the UK DBT. Again, the RP recognises this as good practice within its submissions but as the safety case is not fully developed at this stage in GDA it has yet been unable to utilise this data.
10. The two approaches for identifying IEMOs and PSES from PIEs contained within, and excluded from, the safety case fully meet my expectations and align with VAI&C RGP. Precisely how this data is used when it becomes available in Step 3 to identify credible sabotage events will be a target of my future assessment activity.
11. In order to provide a demonstration of its Phase 2b methodology the RP had adopted a third approach of identifying IEMOs and PSES. This has been through the VAI&C workshops held with designers and operators to identify malicious actions capable of challenging nuclear safety functions. These workshops have been successful in identifying what I judge to be a reasonable set of IEMOs for the reactor pools. Around 40 IEMOs are detailed in Table 11 of the analysis (ref. [70]), one example for the purposes of this report being the ’sabotage of the cooling chain in the spent fuel pool’. PSES are less well developed at this stage due to the maturity of safety case development.
12. From the IEMOs generated by the workshop SMEs, potential targets are identified which are detailed in Table 12 of the submission, one example being the Spent Fuel Pool Cooling System (SFPCS) and its duplicate trains. This information allows for specific target locations to then be recorded which may later be categorised as vital areas.
13. The three methods chosen by the RP to identify IEMOs described above fully meet my expectations and align with VAI&C RGP. The RP acknowledges that due to the current maturity of the safety case it has been unable to provide a full demonstration of these methods at this time. However, the planned processes described to extract the necessary information from the safety case appear robust. Where the RP has been able to provide a demonstration of its proposed methods, i.e., through SME workshops, the evidence presented shows these to have identified a reasonable set of IEMOs along with potential targets and target locations. I judge this to be a very effective step in its methodology which contains all of the attributes necessary to meet its intended objective.
14. Phase 3a. The purpose of this Phase is to take the initiating event and potential target set data from Phase 2b and apply the UK DBT to determine whether the threat could credibly, and successfully, compromise the functionality of those targets or directly disperse NM/ORM. Where it is judged that target compromise is beyond the threat capability, this is recorded, and those targets excluded from further analysis.
15. For this aspect of its trial study the RP opted for continued use of an alternative DBT to the one applicable to the UK civil nuclear industry. This was despite earlier concerns being raised by ONR and assurances from the RP that the UK DBT would be used throughout the rest of Step 2. The reason provided for the continued use of an alternative threat was to reduce the protective security marking of the RP’s documentation. The application of the UK DBT was also considered to be nugatory work whilst aspects of the design remain under development.
16. I judge the use of an alternative DBT to represent a shortfall. The DBT document is the cornerstone input to any VAI&C analysis as it sets out the hazards against which security risk is determined. Applying an alternative set of hazards to those applicable to the UK results in any VAI&C analysis using that alternative DBT being of no relevance in the UK context. Applying an alternative set of hazards has actually resulted in the work carried out by the RP in Step 2 being nugatory as it will need to be repeated using the correct set of hazards at a later stage.
17. Despite the regulatory concerns raised above, the intent of objective two of Step 2 of this GDA from a VAI&C perspective was for the demonstration of application of the RP’s methodology. My assessment concludes that a reasonable process is in place to assess the capability and credibility of a DBT to prosecute targets. The RP has used engineering judgement to inform this phase to either discount or include target sets for further analysis. The results of the RP’s Phase 3a analysis are recorded in Table 13 of the submission and, although decisions are based on an unrepresentative set of threats, the results appear reasonable for the purposes of demonstrating application of approach only. The results themselves are considered inadequate.
18. This phase will be an area for focused assessment in Step 3 to judge the adequacy of application of the UK DBT by the RP. Use of an alternative DBT in Step 3 will result in any related VAI&C analysis being invalid for UK use as is the case for the output of this trial study for the reactor pools. Use of an alternative DBT in Step 3 will be considered a significant shortfall and raised as such at the beginning of the Step.
19. This phase presented the RP with the opportunity to demonstrate the breadth of its methodology in terms of considering the full range of threat vectors set out in RGP. I consider there to have been sufficient demonstration, for Step 2 of GDA, of direct and indirect attack from Type 1 (onsite) attack vectors. Type 2 (off-site) attack vectors will need to be considered further in Step 3 and I judge that perhaps the reactor pools were not the ideal set of SSCs against which to demonstrate the entirety of a VAI&C methodology. If the process were to be repeated, I would expect demonstration to be through a more complex set of interdependent SSCs directly supporting the reactor FSFs, not the spent fuel pools.
20. Phase 3b. It is in this phase of the methodology where the credible target sets and their locations are categorised for sabotage, by means of radiological consequence analysis, using the graded approach. The submission offers four examples of high-level analysis being carried out to estimate dose consequence noting that additional information, not yet available from the safety case, will be required to verify such results in Step 3. Based on available data at this time, coupled with early inventory assumptions, each of the examples presented lead to a categorisation of High Consequence Vital Area (HCVA). The final set of analysis is tabulated (Tables 6, 7 and 8 of (ref. [70])) in a format showing the FSF being challenged, the list of targets (SSCs) which could lead to the URC if challenged and the locations of those SSCs requiring protection. The specific locations are then categorised for sabotage. I judge this general approach to be satisfactory and to align with VAI&C RGP.
21. Phase 4. This phase presents the identified vital areas in pictorial format on plot plans utilising the available general site layout data. At this stage identified locations are indicative only and are subject to change as the design develops and is refined, which is as I would expect. However, I judge that the finalised plot plans showing confirmed vital area locations at the end of GDA will be of significant value to any future UK licensee.

#### Section conclusion

1. This section of my assessment covered objective two of my VAI&C assessment strategy which was the demonstration of adequacy of the RP’s arrangements through a trial study. In general terms I am satisfied with the information presented given the lack of maturity of the design data available in Step 2 to inform its VAI&C analysis. This has limited the RP’s ability to provide a complete and comprehensive demonstration of its methodology, however, where gaps in information have been identified commitment has been made to carry out further analysis once that information becomes available. This is particularly relevant to Phase 2b which utilises the PSA and FS analysis to directly inform the identification of IEMOs and PSES. Until this safety case analysis becomes available in Step 3 the RP is unable to evidence precisely how it will utilise that safety data for security risk analysis purposes. Due to this being a fundamental building block for VAI&C for NPPs this will be a target for regulatory assessment in Step 3.
2. One key observation raised during my assessment was the exclusion of cyber security expertise from the panel of SMEs. Representation in this area is critical for VAI&C to ensure the accurate identification of URC pathways through blended attack vectors. The RP has provided assurance that cyber expertise will be represented at all future Step 3 workshops. Integration of cyber security into the VAI&C processes will be an area of regulatory focus in Step 3.
3. A key shortfall has been identified which centres around the use of an alternative DBT as opposed to the one setting out the hazards applicable to UK NPPs. The UK DBT document is the cornerstone input to any VAI&C analysis as it sets out the hazards against which security risk is determined. Applying an alternative set of hazards to those applicable to the UK results in any VAI&C analysis using that alternative DBT being of limited relevance in the UK context. This analysis will therefore need to be repeated using the correct set of hazards at a later stage. Further use of an alternative DBT in Step 3 would represent a significant shortfall.
4. Claims are presented within the submissions around the behaviour of particulate following highly energetic dispersal events within containment structures. These claims will require further substantiation, in accordance with ONR SAP AV series, and will be a particular target for regulatory focus in Step 3.
5. I am satisfied that each of the key components of a VAI&C methodology are present, albeit in some cases the order in which they have been applied requires additional focus by the RP. I will continue to engage on this during GDA to seek a resolution.
6. Overall, noting the topics requiring follow-up action above which are largely the result of a less well-developed design than anticipated at this point in GDA, I am content that the RP has sufficiently met the intended VAI&C objectives of Step 2 of this GDA.

### Cyber Security

#### Introduction

1. As the first substantial technical assessment step, ONR’s expectations for Step 2 are that the RP should demonstrate their approach to analysis of cyber risks to the design by identifying, characterising and assessing the relevant systems to demonstrate they can be appropriately protected. This is in order to protect the public from risks arising from theft and sabotage of NM and ORM and supporting systems by means of cyber attack.
2. The focus of my assessment was the fundamental adequacy of the methodology and a demonstration of its application against the design. This would allow the RP to demonstrate in GDA that cyber security risks to the design will be identified and assessed to inform the design of a CPS as part of the overall security justification. This should take into account the cyber threats described in the UK DBT (ref. [24]) and demonstrate the relevant CPS outcomes defined in SyAPs can be met (ref. [69]).
3. My assessment in this section was based on the following submissions:

* The Cyber Security Risk Assessment Methodology (CSRAM) (ref. [72])
* The Cyber Security Risk Analysis (ref. [61])
* The Cyber Security Report (ref. [62])

1. In making my assessment, I also made reference to the RP’s Threat Interpretation (ref. [48]), Security Functional Categorisation and Classification (ref. [49]), the Secure by Design Methodology (ref. [50]), the Secure by Design Report (ref. [52]), the C&I Safety and the Cyber Security Integration Strategy (ref. [68]).

#### Cyber Security Risk Assessment Methodology

1. The RP’s CSRAM sets out a process to identify, assess and manage cyber risks through the lifecycle of the design and operation of the Rolls-Royce SMR (ref. [60]). My expectation was for a methodology that sets out a clear, coherent and repeatable process for identification, assessment and management of potential cyber security risks to the design. I expected the methodology to draw from appropriate standards and RGP to demonstrate application of the KySPPs and provide a credible means of meeting the outcomes for a CPS via the application of a comprehensive set of controls. In line with the RP’s scope and design philosophy, I expected the methodology to incorporate the SbD approach and an understanding of safety requirements (in regard to CBSIS) to allow early identification of design requirements. I initially assessed Issue 1 of the methodology (ref. [72]) and raised two RQ’s (RQ-01052 and RQ-01053, ref. [67]), with the RP incorporating my feedback into Issue 2.
2. The methodology consists of a seven-step process based around the IEC 62443-3-2 standard for Security Risk Assessment for System Design (ref. [34]). The security levels from that standard have been substituted with the security degrees from IEC 62645 (ref. [36]) which allows for security control requirements to be graded to the nuclear safety significance of a particular system. The methodology integrates threat intelligence from the Threat Interpretation submission (ref. [48]) and leverages the tactics and techniques from the MITRE ATT&CK framework to structure a detailed assessment of risks (ref. [73]). Control sets are provided which are based on the system security requirements from IEC 62443-3-3 (ref. [35]) and the security degree requirements from IEC 62645 as well as the related controls in IEC 63096 (ref. [74]).
3. I found the high-level process to be clear and demonstrated alignment with Clause 4 of the IEC 62443-3-2 standard, i.e., the primary steps of conducting an iterative cyber security risk assessment incorporating system identification, an initial risk assessment of a system, partitioning it into zones and conduits and then conducting a detailed assessment dependent on the risk which then informs the controls selected. It is clear how the separate assessment of threats (the Threat Interpretation) interfaces with the process. I considered that the innovative approach taken allows for modelling and analysis of adversary attack paths to systems. These are increasingly part of RGP and my expectations for demonstrating the efficacy of a CPS, particularly in regard to demonstrating that a URC cannot be achieved by a cyber attack within the capability described in the UK DBT.
4. I judged the submission demonstrated good understanding of UK government risk appetite and regulatory expectations within SyAPs for achieving specified security outcomes. I found it to be comprehensive in addressing the scope of what such a methodology should encompass and the selected standards, techniques and RGP are judged to be suitable for the intended purpose. Internationally recognised standards for generic OT cyber security are combined with those specific to nuclear C&I, in line with my expectations. The interfaces with other processes and the golden thread from the overall security claim through identification, assessment and into requirements was clear.
5. I found that a number of changes had been made in response to the feedback provided and addressed the clarifications requested in my RQs (ref. [67]). The RP clarified the relationship between the risk tolerance and the CPS outcomes. They introduced controls that would apply to all systems in scope as part of a revising its overall approach to grading risks. Combined with the applicability of security degrees based on categorisation and classification for both CBSIS and CBSy, I judge this should allow the appropriate systems to be assessed and controls implemented to demonstrate a graded approach to CPS design. While the relationship to the CPS outcomes was outlined and it was made clear they will be demonstrated, it would increase confidence to understand further how this will be described (given the limitations in the trial analysis described below).
6. The annex of security controls included those from IEC 63096 as the companion control set to IEC 62645 in addition to those control sets previously included in Issue 1 (which mostly drew from IEC 62443-3-3). While this inclusion was logical and consistent with the security degree approach, it meant that there were several control sets that were referenced, rather than the good practice of identifying a core set which could be supplemented to meet the RP’s requirements. I judged the overall approach to the controls to be insufficiently clear and requiring further refinement. The RP needs to ensure a comprehensive set of controls is defined in line with regulatory expectations and consistent with the selected standards. The RP subsequently committed to addressing this in response to an RQ I raised regarding the subsequent trial analysis (RQ-01215, ref. [67]).
7. The methodology included a separate process to address assessment of attacks affecting multiple systems. I judged this needed further refinement to distinguish this analysis from existing assessments for functional safety and account for the foreseeable actions of a malicious attack. In response to a subsequent RQ (RQ-01215, ref. [67]), the RP committed to address this in a future revision of the methodology.
8. The approach to defining zones and conduits defined the ‘System Under Consideration’ to be individual CBSIS and CBSy which would mean that division into zones would be done on an individual system basis. While there could be benefits from this approach, I note it potentially does not reflect the original intent of the standard which seeks the zones and conduits to be applied at a higher level of the architecture which I judge would have greater benefit to ensuring the design is appropriately segregated on the basis of overall risk with appropriate controls applied (however this approach would benefit from increased design maturity). I will seek further clarity on the RP’s approach to zoning for the higher level Reactor Island C&I architecture in Step 3.
9. The methodology also contained an assumption that CBSIS would not have any connectivity to a licensee’s Enterprise network and thus these types of risk would only be assessed once any connectivity had been identified. Given the potential implications for the GDA scope and meaningfulness of the assessment, this was an aspect I sought to clarify with the RP after my assessment of the trial analysis (RQ-01214, ref. [67]).
10. I assess that the CSRAM meets expectations for Step 2 of GDA in that the methodology is fundamentally adequate. The methodology is based on RGP and appropriate standards, capable of demonstrating the relevant outcomes and incorporates the relevant KySPPs in the approach. The approach to CBSIS aligns with the broad principles for protection of C&I systems set out in IAEA NSS-33T (ref. [29]). That is, one based on the application of a graded approach incorporating security levels/degrees and zones and identifying security requirements during the design phase. It is also consistent with supporting defensive computer security measures and architecture in line with IAEA NSS-17T (ref. [27]). However, there are some aspects from my assessment, taking into account the outcomes from the trial analysis (see below), which I judge require further development and refinement to increase my confidence in the assessments to be conducted in Step 3.

#### Cyber Security Risk Analysis

1. The RP produced a Cyber Security Risk Analysis submission which provided the results from a trial of the CSRAM against two Reactor Island C&I systems (ref. [61]).
2. My expectations for the trial were that it would demonstrate the application of the methodology, identify any improvements needed and provide early identification of design requirements to help realise the RP’s intent of SbD. I was looking for a demonstration that an appropriate range of risks were identified, and suitable controls applied to reduce risk as well as the overall functioning of the methodology against expectations. I was also looking for evidence of joint working with the C&I design team in terms of understanding safety functions and consequences of system compromise. Recognising the relatively low maturity of systems at this stage of the design, I was expecting caveats on the analysis to be applied and any assumptions made to be justified with a view to giving a clear sense of the approach to subsequent analysis in GDA. Finally, I expected clear articulation of any risks identified in order to feed into requirements for the design and constructive review of any improvements required in the methodology and its application.
3. The trial analysis was conducted against two candidate SSCs which were selected due to their safety significance and relative design maturity:

* The Diverse Protection System (DPS) [JQA], a class 1 system that provides a diverse primary means of implementing category A safety protection functions.
* The Reactor Protection System (RPS) [JRA], a class 2 CBSIS system that provides a secondary means of implementing all category A safety protection functions and a primary means of implementing category B protection functions.

1. An early design decision and application of SbD (ref. [51]) meant that the DPS will be based on non-programmable technology and thus insusceptible to direct cyber attack once in operation. However, the monitoring subsystem (the DPSMS) is a class 2 system which is assumed to be digital and programmable and hence it was considered necessary to analyse. The RPS is based on digital, programmable technology.
2. I found that the RP had placed several caveats on the trial analysis. As expected, the trial was limited by the design maturity of the systems and a lack of detailed information to inform assessment of vulnerability. While the Detailed Assessment step of the CSRAM was conducted, the RP chose not to claim a reduction in the residual risk to the systems after applying the controls as it was felt there was insufficient basis to do so (with the exception of the hardwired DPS). Similarly, there was insufficient confidence from the RP to provide the CPS outcomes justification at this stage. However, the RP was able to demonstrate application of the Threat Interpretation (ref. [48]), defining sabotage actions, showing the analysis within the MITRE ATT&CK framework of applying the resultant techniques and tactics against the systems and considering the relevant consequence level. The RP also demonstrated an indicative division of the systems into zones though this was based on a granular sub-division of the individual systems (rather than referring to any higher level architecture design).
3. I found that, despite identifying some potential security risks, the trial did not articulate formal requirements for the design as a result of the analysis. A potentially significant risk in connectivity between systems was identified in the narrative of the report, and potential mitigations suggested, but then not formally identified as an early requirement or action. The objective of the analysis from the RP (and my expectation) suggested requirements would be identified as a result of the trial. However, the RP concluded the analysis by stating it would conduct the assessments again with a more developed version of the methodology, benefiting from increased design maturity. I found there to be a limited set of recommendations for when the analysis was repeated.
4. I also found there to be some aspects of the analysis that represented potential shortfalls against my expectations for system assessments. Some assumptions made around the safety impact of system compromise were not reflective of the safety classification, suggesting that the relationship with the safety case and coordination with the C&I design team needed to be improved. I also found that some potentially significant assumptions about system vulnerability and attacker capability were made and not justified. Similarly, some claims on inherent controls in the design were made on the basis of safety segregation but not justified in terms of security (though it is accepted the relatively low design maturity made this challenging). The analysis also used an indicative version of the control sets as provided in the CSRAM (pending further work by the RP), preventing a full assessment of the controls applied, with my sampling identifying some potential gaps to the standards referenced.
5. As a result of my assessment I raised an RQ in conjunction with the C&I topic that sought further information on how the RP intended to address the issues identified with the analysis and to clarify the RP’s arrangements for the conduct and documentation of subsequent assessments (RQ-01215, ref. [67]). The RP provided a comprehensive response, confirming that a further issue of the methodology would be produced early in Step 3 to take account of the feedback provided.
6. I found the analysis from the trial had also minimised or discounted the risks from onward or remote connectivity based on an assumption that connectivity with an enterprise network would not exist or be assessed outside of GDA. As noted above, Issue 2 of the CSRAM also included this assumption. I raised an additional RQ to request clarification of the GDA scope and confirm that such risks would be addressed in the analysis (RQ-01214, ref. [67]). The RP confirmed that such risks would be addressed via CSRAM assessments, and the methodology updated accordingly. However, the RP did not clarify the difference with the stated GDA scope, only confirming that CBSIS and CBSy would be subject to assessment. This is an aspect I will seek to clarify in Step 3 to ensure the detailed scope and the assumptions being made are understood.
7. The RP also provided a demonstration of the treatment of cyber security risks using the core SbD methodology (ref. [51]) against the class 1 DPS, offering further evidence of the SbD approach as well as the role of C&I design rules and prior work on OT security in determining requirements. This demonstration was also limited by design maturity though recommendations for improving risk reduction for cyber security were made. Consistent with the C&I assessment (ref. [38]), it should be highlighted that the decision to design the DPS around hardwired, non-programmable technology is judged to considerably reduce the overall cyber risk in relation to a URC and provides early evidence of the SbD philosophy by the RP.
8. In summary, the trial analysis provided a limited demonstration of the methodology. However, it did enable some key aspects to be evidenced and allowed the RP to identify improvements with a clear commitment to addressing shortcomings and gaps in response to my feedback. The RP subsequently clarified that they would be conducting a full analysis of both systems again prior to them reaching greater maturity which would allow cyber security requirements to be reflected in the design of CBSIS in scope (prior to being subject to formal design change processes) (ref. [3]). This should allow the RP to demonstrate the application of their processes to achieve a level of SbD based on a full application of a further revision of the CSRAM. Though I expected a more comprehensive demonstration in terms of identifying requirements within Step 2, it should be acknowledged that it is a positive and beneficial move that security requirements are being considered at this early stage of the design. The challenges in providing a comprehensive assessment (particularly around connectivity) at the current design maturity is also recognised.
9. Overall, taking into account the response to my feedback, the commitment to address the issues identified, and recognising the challenges of the design maturity, I am satisfied with the information presented in Step 2.

#### Cyber Security Report

1. The RP submitted their Cyber Security Report (CSR) for assessment (ref. [62]). The CSR is a Tier 2 document which records the cyber security analysis work performed to date, discusses the results of the Step 2 activities and provides CAE related to cyber security. The report made a number of recommendations for activities in Step 3 and sets out the RP’s intent for improving the application of the CSRAM process. Further versions of this report will be issued in Step 3 to inform development of the ISS (including specification of a CPS).
2. I found the CSR adequately described the RP’s approach to addressing cyber security risks in Step 2 and the findings and recommendations broadly reflected my feedback and the RQs raised as a result of the trial analysis. The limitations of the CSRAM trial and caveats on the outputs of the analysis were generally well recognised and there is clear identification of how the RP intends to address this in Step 3.
3. Notably, the more significant risks identified in the trial were summarised, and while I identified some gaps to what was identified in the trial, it provided a demonstration of risk articulation that I assessed had been missing from the trial analysis. As such I judge that while the RP was unable to fully demonstrate the application of the CSRAM in identifying cyber security requirements for the C&I design in Step 2, they have provided sufficient confidence that this will be demonstrated at an appropriate stage in the design process in Step 3 and is thus adequate for this step.
4. The report made a commitment to issue a further issue of the CSRAM to address some of my concerns identified in the trial and highlighted in my feedback. Notably, the RP would fully align the control sets with their chosen standards which should ensure these are comprehensive and appropriate to managing the risks to CBSIS in line with RGP. Other aspects referenced in the RP’s response to my trial analysis RQ were addressed to my satisfaction in the CSR (RQ-01215, ref. [67]).
5. Additionally, while the RP has provided information on its broad approach to assessment of risks that could be introduced during systems development of CBSIS and CBSy, it still lacks a strategy for demonstrating Production Excellence and definition of an appropriate set of Independent Confidence Building Measures for cyber security. The CSR includes a commitment to develop such a strategy for security, noting that similar commitment has been made by the RP’s C&I design team (ref. [38]).
6. I judge that the CSR provides an adequate summary of the RP’s cyber security activities to date and provides the necessary commitments to future analysis against the design and improvements to their processes and documentation.

#### Section conclusion

1. Based on the outcome of my assessment, I judge that the RP’s approach to identification, assessment and mitigation of cyber risks to the design is consistent with that outlined in SyAPs, IAEA guidance and other RGP. The RP’s methodology for assessment of cyber risks is judged to be adequate with an approach informed by SbD, the threat and is capable of demonstrating CPS outcomes via application of the graded approach to CBSIS and CBSy. However, the methodology will require further refinement in Step 3 and the RP is committed to continuous improvement. Nonetheless, the trial provided only a partial demonstration of the functioning of the methodology and offered limited evidence of SbD. While not undermining my judgement for Step 2, this will require further attention in Step 3.
2. Therefore, my assessment has identified a number of aspects for the RP to develop in Step 3. I will also continue to liaise closely with the C&I assessor to resolve the issues identified in support of the safety objectives in respect to cyber security.
3. I am content that the RP has met the Cyber Security objectives of Step 2 of this GDA. The RP has met my expectations in the relevant submissions and commitments to further development of its methodology and related processes.

### Integrated Security Solution

1. Due to limitations around design maturity within Step 2, the RP submitted an early version of their ISS document at the end of the step (ref. [63]). Whilst a detailed assessment will take place within Step 3, it was my expectation during Step 2 that the RP be able to describe what they are aiming to achieve at the end of GDA in terms of a security regime. Essentially a sufficiently developed PPS and CPS so to provide a future licensee with a basis for developing a NSSP. Furthermore, that the RP should be able to provide assurances that the eventual security design is informed by proven risk assessment methodologies and the application of SbD, meeting regulatory expectations.
2. The ISS has provided me with a valuable picture of what the RP aims to achieve in GDA and what aspects of the security regime will become the responsibility of the eventual licensee. The RP explained that a detailed description of operational requirements for security is out of scope, as these would be potentially outdated due to the fluidity of design and advances in technology through later development. I recognise and accept that the RP is in a unique position of applying processes with the aim of building a security posture whilst the reactor is being designed. Nevertheless, the RP’s considerations regarding the ISS provide me with confidence that the ‘so what’ for Step 3 is being considered within Step 2. Positively, the RP explained that a ‘security integrator’ would be appointed to facilitate this transition during handover to a licensee.
3. The RP has explained how it is developing the ISS. This included acknowledgement of RGP, regulatory outcomes as described within SyAPs and the recognition that the ISS would provide a basis for the subsequent development of an NSSP. The RP understood that the latter would require ONR’s approval after GDA. The RP went on to explain how the ISS would be created using their engineering process and within the development of the design. I assess that the RP’s explanation at this stage meets my expectations.

# Conclusions

* 1. Conclusions

1. This report presents the Step 2 security assessment for the GDA of the Rolls-Royce Small Modular Reactor. The focus of my assessment in this step was towards the fundamental adequacy of the design and security case. I have assessed the Tier 1 E3S chapters and relevant supporting documentation provided by Rolls-Royce SMR Limited to form my judgements. I targeted my assessment, in accordance with my assessment plan (ref. [64]), at the content of most relevance to security against the expectations of ONR’s SyAPs, TAGs and other guidance which ONR regards as RGP.
2. Based upon my assessment, I have concluded the following:

* The assessment has been completed of the relevant submissions in line with the Step 2 objectives and my assessment plan. The quality of submissions met my expectations. The topics for Step 2 have been covered in a comprehensive manner drawing from RGP and also informing evolving security thinking on SbD that offers benefits to a developer.
* I judge that the GSR ‘header’ document provides a comprehensive framework on which to build on in Step 3. The RP has adopted an ambitious approach to developing a security case. First, the security case is integrated into a wider E3S case. Secondly, their approach to SbD, as a security-wide ‘philosophy’ along with its practical application, offers ways to influence the design for security benefit.
* Integrated working with their designers and engineers has been evident although not necessarily fully effective given this is a new organisation.
* The security ‘narrative’ is an intelligent one that reflects a SyAPs based approach. The RP’s overall security case development also seeks to integrate cyber security into wider security risk management and reaches outside security especially to C&I.
* The RP has focused correctly on identifying risks to the design. While design maturity has been a limiting factor, the RP has developed workable methodologies for determining and managing security risks.
* The RP has sufficiently met the intended VAI&C objectives for Step 2. It has developed a set of arrangements which, through a trial study, I consider to have demonstrated a satisfactory level of alignment with UK and international RGP. However, the design maturity has limited the availability of the design data to enable the RP to provide a complete and comprehensive demonstration of its arrangements at this time. In addition, the RP must ensure it uses the UK DBT in Step 3.

* The RP has met the intended cyber security objectives for Step 2. They have improved their methodology and sought to apply it at an early stage of design maturity. While I expected to see a more complete demonstration of the methodology, and there are aspects which will require further improvement, the RP has provided a good foundation for Step 3.

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

## Recommendations

1. My recommendations are as follows:

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

References

|  |  |
| --- | --- |
| [1] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction, SMR0004294, Issue 3, May 2024. (Record ref. ONRW-2019369590-9881). |
| [2] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 2: Generic Site Characteristics, SMR0004542, Issue 3, May 2024. (Record ref. ONRW-2019369590-9883). |
| [3] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 32: Generic Security Report, SMR0004682, Issue 3, May 2024. (Record ref. ONRW-2019369590-9905). |
| [4] | 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. |
| [5] | ONR, Security Assessment Principles for the Civil Nuclear Industry. 2022 Edition, Version 1, March 2022. www.onr.org.uk/media/g05fszjn/security-assessment-principles.pdf. |
| [6] | ONR, Technical Assessment Guides. www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/technical-assessment-guides-tags/nuclear-security-tags/technical-assessment-guides-tags-nuclear-security/. |
| [7] | ONR, Guidance on the Production of Reports for Permissioning and Assessment, NS-TAST-GD-108, Issue No. 1, December 2022. (Record ref. 2022/71935). |
| [8] | 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. |
| [9] | ONR, Step 2 Topic Assessment Plan for the Generic Design Assessment of the Rolls-Royce SMR, ONR-GDA-AP-22-022, Issue No. 1, March 2023. (Record ref. ONRW-2126615823-784). |
| [10] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 summary, ONRW-2019369590-8980, Issue No. 1, July 2024. (Record ref. ONRW-2019369590-8980). |
| [11] | Rolls-Royce SMR Limited, Rolls-Royce SMR Generic Design Assessment Scope, SMR0002183, Issue 2, January 2023. (Record ref. ONRW-2019369590-8058). |
| [12] | Rolls-Royce SMR Limited, GDA Scope and Submission Plan for Nuclear Security, SMR0003259, Issue 1, November 2022 (Record ref. 2023/7989). |
| [13] | ONR, Safety Assessment Principles for Nuclear Facilities (SAPs), 2014 Edition, Revision 1, January 2020. www.onr.org.uk/media/pobf24xm/saps2014.pdf. |
| [14] | IAEA, Safety Standards. www.iaea.org. |
| [15] | IAEA, Nuclear Security series. www.iaea.org. |
| [16] | ONR, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs, CNSS-TAST-GD-11.1, Issue 1.2, 2021. www.onr.org.uk/media/documents/guidance/cnss-tast-gd-11.1.pdf. |
| [17] | ONR, ONR Technical Assessment Guide: Effective Cyber and Information Risk Management, CNS-TAST-GD-7.1, Issue 2, March 2023. www.onr.org.uk/media/documents/guidance/cns-tast-gd-7.1.docx. |
| [18] | ONR, ONR Technical Assessment Guide: Protection of Nuclear Technology and Operations, CNS-TAST-GD-7.3, Issue 2, March 2022. (Record ref. 2022/6881). |
| [19] | ONR, ONR Technical Assessment Guide: Categorisation for Theft, CNS-TAST-GD-6.1, Issue 2, March 2023. www.onr.org.uk/media/documents/guidance/cns-tast-gd-6.1.docx. |
| [20] | ONR, ONR Technical Assessment Guide: Categorisation for Sabotage, CNS-TAST-GD-6.2, Issue 2, June 2023. www.onr.org.uk/media/documents/guidance/cns-tast-gd-6.2.docx. |
| [21] | ONR, ONR Technical Assessment Guide: Radiological Analysis for Fault Conditions, NS-TAST-GD-045, Issue 7, April 2024. www.onr.org.uk/media/documents/guidance/ns-tast-gd-045.pdf. |
| [22] | ONR, ONR Technical Assessment Guide: Physical Protection System Design, CNS-TAST-GD-6.3, Issue 2, March 2023. (Record ref. 2019/135667). |
| [23] | ONR, ONR Technical Assessment Guide Secure by Design, CNS-TAST-GD-11.4.1, Issue 1.1, January 2023. www.onr.org.uk/media/documents/guidance/cns-tast-gd-11.4.1.docx. |
| [24] | HM Government, UK Design Basis Threat, April 2023, (OFFICIAL SENSITIVE – hard copy only). |
| [25] | IAEA, Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC-225, Revision 5, January 2011. www.iaea.org. |
| [26] | IAEA, Identification of Vital Areas at Nuclear Facilities, Nuclear Security Series No. 16, November 2012. www.iaea.org. |
| [27] | IAEA, Computer Security Techniques for Nuclear Facilities, Nuclear Security Series No. 17-T (Rev. 1), September 2021. www.iaea.org. |
| [28] | IAEA, Engineering safety aspects of the protection of nuclear power plants against sabotage, Nuclear Security Series No. 4, January 2007. www.iaea.org. |
| [29] | IAEA, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Nuclear Security Series No. 33-T, May 2018. www.iaea.org. |
| [30] | IAEA, Handbook on the Design of Physical Security Protection Systems for Nuclear Material and Facilities, Nuclear Security Series No. 40-T, May 2021. www.iaea.org. |
| [31] | IAEA, Preventive and Protective Measures Against Insider Threats, Nuclear Security Series No. 8-G, January 2020. www.iaea.org. |
| [32] | The Institution of Engineering and Technology, Code of Practice: Cyber Security and Safety, 2021. https://electrical.theiet.org/guidance-and-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/). |
| [33] | BSI, BS ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection. Guidance on managing information security risks, October 2022. knowledge.bsigroup.com. |
| [34] | BSI, BS EN IEC 62443-3-2:2020 Security for industrial automation and control systems Part 3-2: Security risk assessment for system design, September 2020. knowledge.bsigroup.com. |
| [35] | BSI, BS EN IEC 62443-3-3:2019 Industrial communication networks – Network and system security Part 3-3: System security requirements and security levels, May 2019. knowledge.bsigroup.com. |
| [36] | BSI, BS EN IEC 62645:2020 Nuclear power plants - Instrumentation, control and electrical systems - Cybersecurity requirements, August 2020. knowledge.bsigroup.com. |
| [37] | BSI, BS EN IEC 62859:2020: Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity, September 2020. knowledge.bsigroup.com. |
| [38] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Control and Instrumentation, ONRW-2126615823-2965, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2965). |
| [39] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Internal Hazards, ONRW-2126615823-3464, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3464). |
| [40] | 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). |
| [41] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Probabilistic Safety Analysis, ONRW-2126615823-2692, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2692). |
| [42] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Radiological Protection, ONRW-2126615823-3184, Issue No. 1, July 2024. (Record ref. ONRW-2126615823-3184). |
| [43] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Life Fire Safety, ONRW-2126615823-3608, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3608). |
| [44] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Electrical Engineering, ONRW-2126615823-3090, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3090). |
| [45] | IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61, September 2021. www.iaea.org. |
| [46] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Chapter 32: Generic Security Report, SMR0004682, Issue 1, March 2023. (Record ref. 2023/21286). |
| [47] | Rolls-Royce SMR Limited, Strategy for Development of a GSR for Rolls Royce SMR, SMR0001611, Issue 2, April 2023. (Record ref. 2023/26311). |
| [48] | Rolls-Royce SMR Limited, Interpretation of Design Basis Threat (DBT), SMR0006961, Issue 1, July 2023. (Report ref. N/A due to classification). |
| [49] | Rolls-Royce SMR Limited, Functional Security Categorisation and Classification Methodology, SMR0005655, Issue 2, September 2023. (Record ref. ONRW-2019369590-4349). |
| [50] | Rolls-Royce SMR Limited, Secure by Design Methodology, SMR0005789, Issue 4, May 2023. (Record ref. ONRW-2019369590-2870). |
| [51] | Rolls-Royce SMR Limited, Secure by Design Analysis, SMR0009049, Issue 1, November 2023. (Record ref. Available via Rolls-Royce SMR Information Exchange). |
| [52] | Rolls-Royce SMR Limited, Secure by Design Report, SMR0009697, Issue 4, January 2024. (Record ref. ONRW-2019369590-7254). |
| [53] | Rolls-Royce SMR Limited, Vital Area Identification & Categorisation Methodology, SMR0006499, Issue 1, June 2023. (Record ref. ONRW-2019369590-3085). |
| [54] | Rolls-Royce SMR Limited, Vital Area Identification Workshop Output, SMR0008757, Issue 1, October 2023 (Record ref. ONRW-2019369590-5573). |
| [55] | Rolls-Royce SMR Limited, Vital Area Identification and Categorisation Analysis, SMR0008452, Issue 1, October 2023. (Record ref. ONRW-2019369590-7496). |
| [56] | Rolls-Royce SMR Limited, Vital Area Identification and Categorisation Report, SMR0009689, Issue 1, January 2024. (Record ref. ONRW-2019369590-6713). |
| [57] | Rolls-Royce SMR Limited, Categorisation of Theft Methodology, SMR0006854, Issue 1, July 2023. (Record ref. ONRW-2019369590-3578). |
| [58] | Rolls-Royce SMR Limited, Theft of Material and Categorisation, SMR0008886, Issue 1, November 2023. (Record ref. ONRW-2019369590-5390). |
| [59] | Rolls-Royce SMR Limited, Theft of Material and Categorisation Report, SMR0009686, Issue 1, January 2024. (Record ref. ONRW-2019369590-6713). |
| [60] | Rolls-Royce SMR Limited, Cyber Security Risk Assessment Methodology, SMR0006431, Issue 2, October 2023. (Record ref. ONRW-2019369590-4862). |
| [61] | Rolls-Royce SMR Limited, Cyber Security Risk Analysis, SMR0008887, Issue 1, November 2023. (Record ref. ONRW-2019369590-5391). |
| [62] | Rolls-Royce SMR Limited, Cyber Risk Assessment Report, SMR0009698, Issue 1, January 2024. (Record ref. ONRW-2019369590-6712). |
| [63] | Rolls-Royce SMR Limited, Rolls-Royce SMR: Integrated Security Solution, SMR0009908, Issue 1, February 2024. (Record ref. ONRW-2019369590-7864). |
| [64] | ONR, Step 2 Security Assessment Plan for the Generic Design Assessment of the Rolls-Royce SMR, ONR-GDA-AP-22-014, Issue 1, March 2023. (Record ref. ONRW2126615823-525). |
| [65] | Rolls-Royce SMR Limited, Rolls-Royce SMR – GDA Design Reference Report, SMR0009043, Issue 2, April 2024. (Record ref. ONRW-2019369590-8872). |
| [66] | Department for Energy Security and Net Zero, Secure by Design – Guidance Document, Principles and Methods, Ref R3.6.07, January 2020. (Available via Rolls-Royce SMR Information Exchange). |
| [67] | ONR, Schedule of Step 2 Regulatory Queries, April 2024. (Record ref. ONRW-2019369590-9071). |
| [68] | Rolls-Royce SMR Limited, C&I Safety and Cyber Security Integration Strategy, SMR0004666, Issue 2, January 2024. (Record ref. ONRW-2019369590-7020). |
| [69] | ONR, Security Assessment Principles for the Civil Nuclear Industry - Classified Annexes, Version 1.1, March 2022. (Record ref. 2021/79032). |
| [70] | Rolls-Royce SMR Limited, Vital Area Identification and Categorisation Analysis, SMR0008452 Issue 2, February 2024. (Record ref. ONRW-2019369590-7496). |
| [71] | Rolls-Royce SMR Limited, SMR-019 – Reactor Island Pools Structural Form – Decision Record, SMR0006990, Issue 1, October 2023. (Record ref. ONRW-2019369590-4776). |
| [72] | Rolls-Royce SMR Limited, Cyber Security Risk Assessment Methodology, SMR0006431, Issue 1, June 2023. (Record ref. ONRW:2029369590-3220). |
| [73] | MITRE Corporation, ICS Matrix v14.0, October 2023. https://attack.mitre.org/versions/v14/matrices/ics/, accessed 26 March 2024. |
| [74] | BSI, BS EN IEC 63096:2020: Nuclear power plants - Instrumentation, control and electrical power systems - Security controls, October 2020. knowledge.bsigroup.com. |

# Appendix 1 – Relevant SyAPs and SAPs considered during the assessment

|  |  |
| --- | --- |
| No. | Title |
| KySPPs | Key Security Plan Principles:  1 – Secure by Design  2 – The Threat  3 – The Graded Approach  4 – Defence in Depth  5 – Security Functional Categorisation and Classification  7 – Codes and Standards |
| FSyP 6 | Fundamental Security Principle 6 - Physical Protection Systems: Dutyholders must implement and maintain a proportional physical protection system that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequence of a successful attack. |
| FSyP 7 | Fundamental Security Principle 7 - Cyber Security & Information Assurance: Dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology. |
| SAP AV.1 | Assurance of validity of data and models. This states that theoretical models should adequately represent the facility and site. |
| SAP AV.2 | Assurance of validity of data and models. This states that calculation methods used for analyses should adequately represent the physical and chemical processes taking place. |
| SAP AV.3 | Assurance of validity of data and models. This states that data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means. |
| SAP AV.5 | Assurance of validity of data and models. This states that documentation should be provided to facilitate review of the adequacy of the analytical models and data. |
| SAP AV.6 | Assurance of validity of data and models. This states that studies should be carried out to determine the sensitivity of the analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation. |