Partner Document Number	Partner Document Issue /Revision	Retention category:
N/A	N/A	A

Title

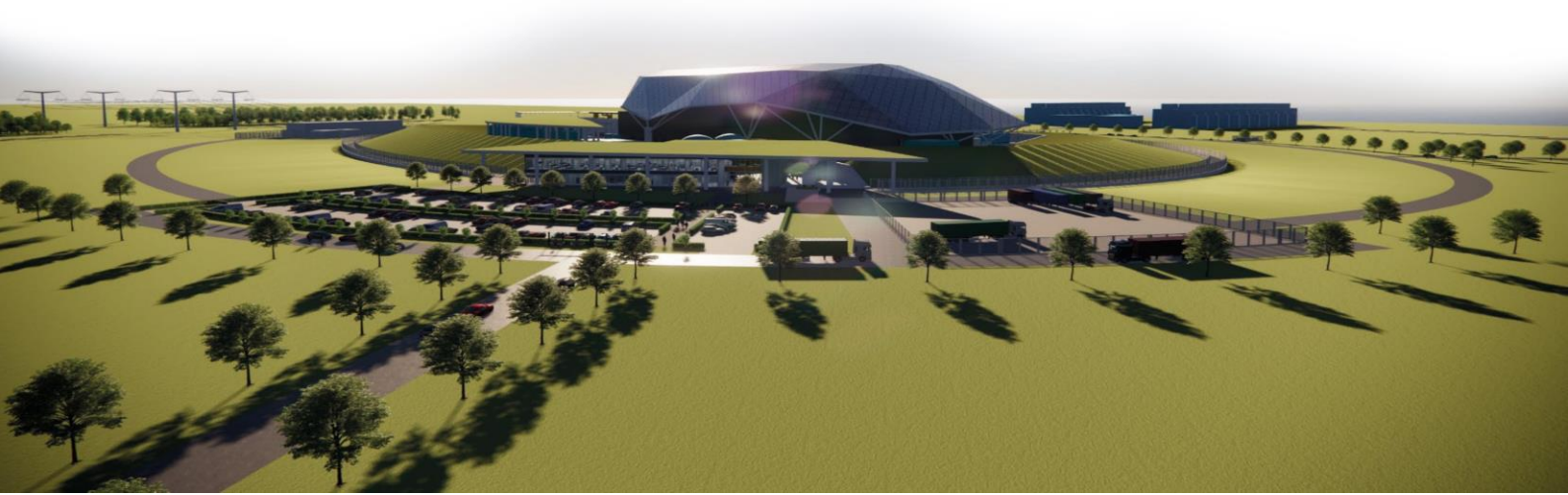
Rolls-Royce SMR Generic Security Report

Executive Summary

The Generic Security Report GSR will present the Security Case for the Rolls-Royce Small Modular Reactor (RR SMR) and it forms Chapter 32 of Rolls-Royce SMR's Environment, Safety, Security and Safeguards (E3S) Case.

The GSR will build-up and (ultimately) replace the Preliminary Security Report (PSyR) that was issued previously.

This revision of the GSR represents the conceptual layout of the document that will be developed by Rolls-Royce SMR throughout Step 2 of the GDA. As such, it presents the framework of the GSR by listing the contents of the document, with a summary at each section to describe how that subject will be developed over the period of Steps 2 and 3 of the GDA. Revision 2 of the GSR will be issued at the end of Step 2 in July 2024.



Contents

Tables

Figures

32.1 Introduction

32.1.1 Introduction

This introductory section of the GSR will be used to 'set the scene' for the report to explain why it has been produced. It is envisaged that it will include the sections outlined below.

32.1.2 Purpose

To explain what the GSR is intending to deliver for the benefit of the maturing Rolls-Royce Small Modular Reactor (RR SMR) and to describe the support that it offers to a future Nuclear Site Licensee (SL) in the development of a Nuclear Site Security Plan (NSSP).

32.1.3 Objectives

A series of objectives will be developed that, once achieved, will enable the GSR to have met its purpose. A preliminary set of security objectives was set out in the PSyR (Reference [1]); these may be further developed as the GSR matures.

32.1.4 Scope

This sub-section will summarise the Structures, Systems and Components (SSCs), and layout, that were considered within the Security Case assessment, and the level of detail that will be used to define the security features to support the regulatory assessment and the SL to design an effective NSSP.

32.2 Delivery of the Environmental, Safety, Security and Safeguards Case

32.2.1 Introduction

This section will describe the benefits of adopting an integrated Environmental, Safety Security and Safeguards (E3S) Case approach, how the case will be structured and how the GSR informs, and is informed by, the E3S Case. It is envisaged to include the following sub-sections:

32.2.2 E3S Case

This sub-section will put the E3S case into context.

E3S Case Strategy - Integrated Approach

This sub-section will describe the strategy adopted and the benefits of an integrated E3S Case.

E3S Case Hierarchy

This sub-section will describe the structure of the case.

Assurance and Safety Case Environment (ASCE) Software

This sub-section will describe the benefits that employing ASCE software will deliver to the case.

GSR within the E3S Case

To describe how the GSR informs, and is informed by, the E3S Case.

32.3 Claims, Arguments and Evidence

32.3.1 Introduction

The development of Claims, Arguments and Evidence (CAE) helps to provide a golden thread through the GSR by providing a framework for the security assessment. The development of this 'golden thread' of CAE 'tells the story' from applying the Office for Nuclear Regulation's (ONR) Security Assessment Principles (SyAPs) (Reference [2]) through to the description of a conceptual design for security in sufficient detail to enable the potential SL to develop that GSR document set into an NSSP.

32.3.2 Fundamental Nuclear Security Claim

The claims, arguments and evidence that will be developed to support the Security Case will emanate from the Fundamental Objective within the E3S Case. This was distilled down into the Fundamental Nuclear Security Claim in the Preliminary Security Report (PSyR) (Reference [1]):

Fundamental Nuclear Security Claim - The nuclear security arrangements for RR SMR will protect people and the environment from harm as a result of malicious actions which could result in Unacceptable Radiological Consequences, the theft of nuclear material and/or the compromise of Sensitive Nuclear Information; this will be achieved through the adoption of internationally accepted standards and recognised 'good practice' as promoted by the IAEA, and will be compliant with the relevant national regulatory regime.

32.3.3 Top Level Security Claims

The Fundamental Security Claims will be decomposed into a set of Top Level (Level 1) claims, which will reflect the primary focus of a nuclear security regime to satisfy regulatory obligations (as outlined in the ONR SyAPs [2]).

A preliminary set of Top Level (Level 1) Security Claims was presented in the PSyR (Reference [1]). These claims covered the topic areas of:

1. Secure by Design
2. Protection from Sabotage
3. Protection from Theft
4. Cyber Security & Information Assurance (CS&IA).

This approach to the development of the GSR mirrors that for nuclear safety, which is typically focussed on the trilogy of 'control of criticality', 'control of heat removal' and 'confinement/containment'.

32.3.4 Security Sub-Claims

As the Level 1 Claims reflect the primary focus of a nuclear security regime, a series of more detailed sub-claims (Level 2 and Level 3) will be developed in the GSR, together with supporting arguments and the evidence to provide a clear path through the Security Case.

The Security Claims (at all levels) will be developed to be suitable to be carried forward into any (UK) Nuclear Site Licence application.

32.4 Generic Security Report

32.4.1 Introduction

The GSR will be presented as a hierarchy of documents that describe the conceptual security design, underpinned by risk-based analysis drawn from Relevant Good Practice (RGP), that might be described as a Security Case and conceptual design requirements. It will summarise the Vital Areas and Operational Technology (OT) that need to be protected within a high level concept of operations, to outline how security risks are designed out and remaining risks are mitigated by designing in security features.

This section is envisaged to comprise the sub-sections outlined below.

32.4.2 Regulatory Framework

The GSR must submit evidence that the proposed design is likely to comply with Nuclear Industries Security Regulations 2003 (NISR) (Reference [3]). It must also demonstrate that regulatory expectations within the ONR SyAPs (Reference [2]) can be met in terms of Fundamental Security Principles (FSyPs), and that all relevant FSyPs have been identified and effective processes are in place to achieve the relevant Key Security Plan Principles (KSyPPs).

It is envisaged that this sub-section will contain direct evidence, or signpost out to where the evidence can be found, for compliance with the following regulatory documents:

1. NISR (Reference [3])
2. SyAPs (Reference [2]) -
    a. FSyPs
    b. KSyPPs.

32.4.3 Relevant Good Practice

The GSR must also justify that the methodologies, approaches, codes, standards and philosophies that it has developed or adopted are based directly or indirectly on source material that is considered to be Relevant Good Practice (RGP). Its analyses should be adequately underpinned by evidence that demonstrates either that RGP or an equivalent standard has been achieved.

The GSR will reference the examples of RGP that it uses, with particular focus on material from:

1. International Atomic Energy Agency
2. Western European Nuclear Regulators Association.

32.4.4 Previous GDA Reports

Relevant guidance from previous GDA security reports will also be considered, alongside the Assessment Reports from ONR.

32.4.5 Structure

The GSR will be structured as a hierarchy of documents that describe the conceptual security design underpinned by risk-based analysis drawn from RGP that might be described as a Security Case and conceptual design requirements.

The Security Case will comprise of a series of tiered documents, as follows:

Tier 1 - This tier will contain the GSR header document as a summary and present the security claims within the Security Case. The GSR will be up-issued, as appropriate, to reflect the maturity of the Safety Case as it develops

Tier 2 – This tier will contain the Methodologies that will be used in the detailed assessments in Tier 3 and provide detailed Topic Reports that draw on information from the Tier 3 assessments. This Tier will present the arguments that support the security claims

Tier 3 – This tier will contain the detailed analysis and assessment reports that will provide the evidence to support the security claims made in Tier 1.

The GSR tiered structure is shown in Figure 32.4-1.

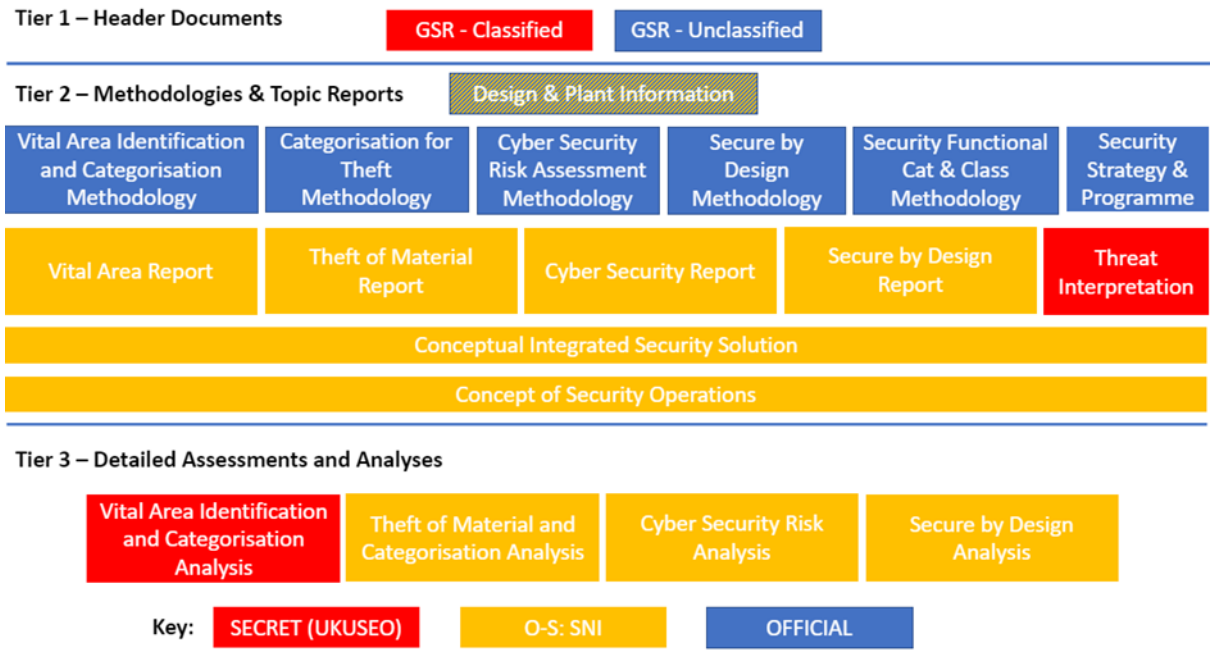


Figure 32.4-1 – GSR Tiered Structure

Tier 1 Head Document:

The Tier 1 Documents are:

1. GSR – Full Version (including classified information)
2. GSR – Redacted Version (excluding classified information).

Tier 2 Documents:

The Tier 2 Documents proposed for issue are:

1. Security Strategy and Programme
2. Vital Area Identification and Categorisation Methodology
3. Categorisation for Theft Methodology
4. Cyber Security Risk Assessment Methodology
5. Secure by Design Methodology
6. Security Functional Categorisation and Classification Methodology
7. Vital Area Report
8. Theft of Material Report
9. Cyber Security Report
10. Threat Interpretation
11. Conceptual Integrated Security Solution
12. Concept of Security Operations.

Tier 3 Documents:

The Tier 3 Documents proposed for issue are:

1. Vital Area Identification and Categorisation Analysis
2. Theft of Material and Categorisation Analysis
3. Cyber Security Risk Analysis
4. Secure by Design Analysis

32.5 Holistic Methodology

32.5.1 Introduction

The development of the full Security Case is a complicated process across multiple topic areas and its integration within the E3S Case. It involves the application of several methodologies and detailed analyses to inform a conceptual integrated security solution. This section will provide an overview of each step within the end-to-end assessment to guide the reader through the Security Case and its interaction with the E3S Case.

It is envisaged that the sub-sections outlined below will be included:

32.5.2 Purpose

This sub-section will set out the purpose and objectives of the Security Case and the approach to its development.

32.5.3 Methodology

This sub-section will provide details of the methodologies and analyses and show how they will be applied and integrated into the overall development of the Security Case.

32.6 Design and Plant Information

32.6.1 Introduction

In support of the Scope of the GSR, this section will identify and describe in more detail the Structure, Systems and Components (SSCs) and plant layout that will be considered in the assessment of the Security Case.

This Section will draw information from the Rolls-Royce SMR Generic Design Assessment Scope and Boundary document (Reference [4]) and the Rolls-Royce SMR Design Overview Report (Reference [5]), with a particular focus on the contents of each that are important to security.

It is envisaged that the section will mirror the structure of the Design Overview Report and therefore contain the sub-sections outlined below.

32.6.2 Scope

This sub-section will summarise the scope of the information presented and provide reference to more informed sources of design information.

32.6.3 Power Station

This sub-section will present the relevant information for this part of the RR SMR.

32.6.4 Reactor Island

This sub-section will present the relevant information for this part of the RR SMR.

32.6.5 Turbine Island

This sub-section will present the relevant information for this part of the RR SMR.

32.6.6 Cooling Water Island

This sub-section will present the relevant information for this part of the RR SMR.

32.6.7 Balance of Plant

This sub-section will present the relevant information for this part of the RR SMR.

32.6.8 Electrical, Control and Instrumentation

This sub-section will present the relevant information for this part of the RR SMR.

32.6.9 Civil, Structural and Architecture

This sub-section will present the relevant information for this part of the RR SMR.

32.7 Threat Interpretation

32.7.1 Introduction

The threat to be applied to the Security Case is mostly defined by the UK Government in the UK Design Basis Threat (DBT) document. The threat is based on an 'intelligent adversary' that acts in a deliberate, planned fashion that is not amenable to a numerical risk estimation. However, it is recognised that the threat definition for the cyber threat is not complete as the threat capability in this subject develops at an ever increasing rate. Therefore, the cyber threat capability will be supplemented with further advice from other Government Agencies such as the National Cyber Security Centre (NCSC).

This section of the GSR will define its interpretation of the physical, cyber and blended threats to the RR SMR. It is envisaged that it will comprise the sub-sections outlined below.

Background

This sub-section will set out the background to the development of the threat interpretation and the sources that have informed it.

Purpose

This sub-section will set out the purposes for which the threat interpretation has been developed.

Scope

This sub-section will set out the scope of the threat assessment that has been developed to inform the Security Case for the RR SMR.

32.7.2 Physical Threat

Threat Intelligence Sources

This sub-section will set out sources that have been used to inform the physical threat.

Adversary Threat Capability

This sub-section will set out the adversary threat capability.

Interpretation of Adversary Threat Capability

An interpretation of the ability of the identified threat (source and capability) to successfully attack the RR SMR will be undertaken.

32.7.3 Cyber Threat

Threat Intelligence Sources

This sub-section will set out sources that have been used to inform the cyber threat.

Threat Assessment Process

This sub-section will set out how the assessment of the cyber threat will be undertaken.

Threat Actors, Sources and Sabotage Acts

This sub-section will set out the scenarios whereby the cyber threat could successfully attack the RR SMR.

32.7.4 Threat Capabilities Removed from Further Assessment

This sub-section will set out the threat capabilities, with rationale, that have been removed from the scope of the security assessment.

32.7.5 Summary of Threat Capabilities

This sub-section will set out capabilities that will be considered within the scope of the security assessment of the RR SMR that will be undertaken.

32.8 Categorisation for Theft

32.8.1 Introduction

It is a regulatory requirement that the GSR identifies appropriate security measures to protect Nuclear Material and Other Radioactive Material (NM/ORM) from theft. The categorisation of the material is linked to the Security Outcomes, Postures and Responses (SORPs) in SyAPs (Reference [2]) used to determine the levels of security that should be applied to protect the material.

This section will describe the methodology adopted by Rolls-Royce SMR to:

1. Identify the NM/ORM that will need security protection from theft
2. Follow the Secure by Design principle to design out security vulnerabilities; categorise the material for theft
3. Minimise the areas that need security protection (against Theft).

The methodology is likely to follow the flow diagram shown in Figure 32.8-1.

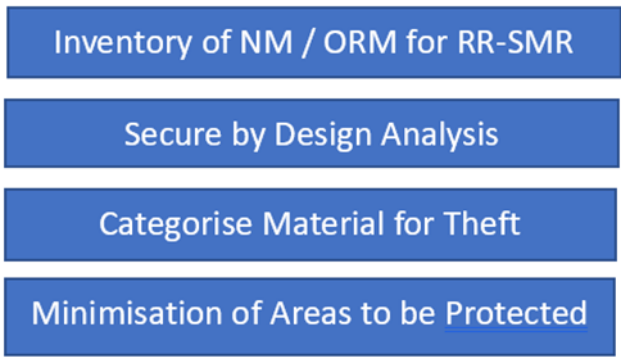


Figure 32.8-1 – Categorisation for Theft Methodology Flow

This section is envisaged to comprise the sub-sections outlined below.

32.8.2 Claims Addressed

This sub-section will set out the Top-Level Claims and Sub-Claims that are to be substantiated by this Section.

32.8.3 Categorisation for Theft Methodology:

Inventory of NM/ORM for Rolls-Royce SMR

This sub-section will summarise the inventory of NM/OR through the life operation of the RR SMR.

Secure by Design Analysis

This sub-section will set out how our Secure by Design approach has attempted to eliminate or substitute vulnerabilities arising from the inventory.

Categorisation of Material for Theft

This sub-section will set out the Categorisation of NM/ORM with regard to theft in accordance with national and international references.

Minimisation of Areas to be Protected

This sub-section will set out where the categorised NM/ORM is co-located material with other elements of the inventory.

32.8.4 Locations Where NM/ORM Will Require Security Protection from Theft.

This sub-section will set out the locations where NM/ORM will require security measure to be put in place as protection from theft.

32.8.5 Outputs from Categorisation for Theft

This sub-section will summarise the outputs from the Categorisation from Theft. These outputs will be passed through to the Conceptual Integrated Security Solution in Section 32.14

32.9 Cyber Security

32.9.1 Introduction

The Security Case for the RR SMR should demonstrate how the Cyber Protection System (CPS) requirements will be met in order to provide protection of nuclear technology and operations. This applies, in particular, to main safety control systems; Computer-Based Security systems (CBSy); and, to Control and Instrumentation (C&I) systems with a focus on Computer Based Systems Important to (Nuclear) Safety (CBSIS).

This section will provide details of the methodology for the assessment of risk of cyber intrusion and malicious action against centralised C&I systems associated with SSCs within the design that could result in an Unacceptable Radiological Consequence (URC) and hence become a Vital Area. It will then summarise how the Secure by Design Principle will be applied to design out vulnerabilities and the security control sets that will be designed into the system to match the CPS Security Outcomes, Responses and Postures (SORPs) that are determine by the consequence of the loss of each system.

An initial Cyber Security Risk Assessment (CSRA) Methodology is shown in Figure 32.9-1.

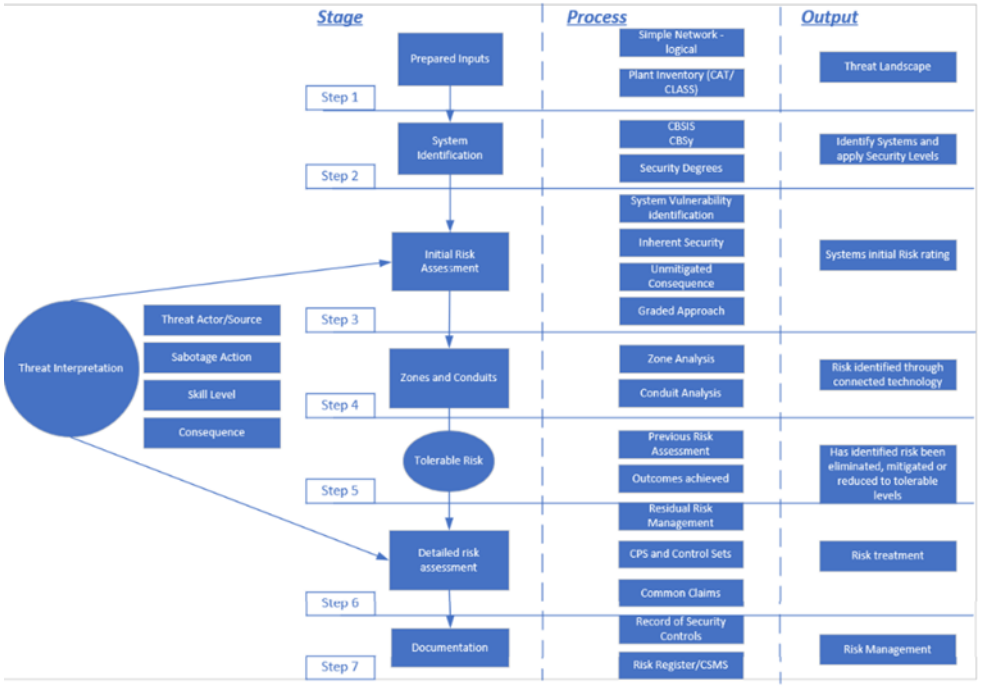


Figure 32.9-1 – Initial Cyber Security Risk Assessment Methodology

The section is envisaged to comprise the sub-sections outlined below.

32.9.2 Claims Addressed

This sub-section will set out the Top Level Claims and Sub-Claims that are to be substantiated by this Section.

32.9.3 Step 1 – Prepared Inputs

These will include simple, logical network diagrams and the safety categorisations and classifications of the plant inventory under consideration.

32.9.4 Step 2 – System Identification

CBSIS and CBSy will form the primary focus of the cyber security risk assessment and this step will identify these systems and allocate appropriate Security Degrees.

32.9.5 Step 3 – Initial Risk Assessment

An initial risk assessment shall be performed to understand the risk rating of each system under consideration.

32.9.6 Step 4 – Zones and Conduits

The systems will be grouped in logical zones with inter-connecting conduits to enable cyber threats to the communication channels to be identified.

32.9.7 Step 5 – Tolerable Risk

To determine whether the initial risk rating for each system is tolerable and meets the CPS SORPs or whether further security measures will be required.

32.9.8 Step 6 – Detailed Risk Assessment

Detailed risk assessment is required when inherent security or previous security Control Sets do not meet the CPS SORPs, and further measures are required.

32.9.9 Step 7 – Documentation

The security controls required by each system to meet the CPS SORPs will be recorded, which may need to be passed onto the future SL.

32.9.10 Outputs from Cyber Security Risk Assessment

The security Control Sets for the C&I, CBSIS and CBSy will be passed through to the Conceptual Integrated Security Solution in Section 32.14. The C&I systems that could contribute to the cause of a URC will be passed into the next section where they will be considered as part of the Vital Area assessment.

32.10 Vital Area Identification and Categorisation

32.10.1 Introduction

One of the central themes to the Security Case is to protect Nuclear Material (NM) and Other Radiological Material (ORM) from sabotage by the threat adversary described in the Threat Interpretation, based on the DBT. Should the act of sabotage lead to a URC, then the material involved in the sabotage attack and the SSCs which maintain the material in a safe condition will be classed as Targets.

The areas in which the Targets are located will be nominated as Vital Areas and these will be categorised into Vital Areas (VAs) or High Consequence Vital Areas (HCVAs) dependent on the level of radiation measured at the site boundary. Areas containing NM/ORM whose sabotage does not lead to a URC will still be identified as they will need security protection as Baseline Areas.

The RR SMR is being designed as it progresses through the period covered by GDA. As a result, not all of the relevant design information is available at this stage to support the security assessment. Therefore, to de-risk the RR SMR design, the Security Case will conduct Preliminary Assumption-based Assessments (PAA) for Vital Area identification and VA/HCVA categorisation.

The initial Vital Area Identification and Categorisation Methodology will be conducted in four phases with frequent opportunities to enter design feedback loops to identify opportunities to apply the Secure by Design Principle and to inform the engineering design of the RR SMR. The initial methodology is shown diagrammatically in Figure 32.10-1.

These four phases are as follows:

1. Phase 1- Preparatory Work
2. Phase 2 - Analysis of Nuclear Inventory and Radiological Consequences
3. Phase 3 – Identify Credible Targets and Categorise Vital Areas
4. Vital Area Location within the RR SMR.

The section is envisaged to comprise the sub-sections outlined below.

32.10.2 Claims Addressed

This sub-section will set out the Top Level Claims and Sub-Claims that are to be substantiated by this Section.

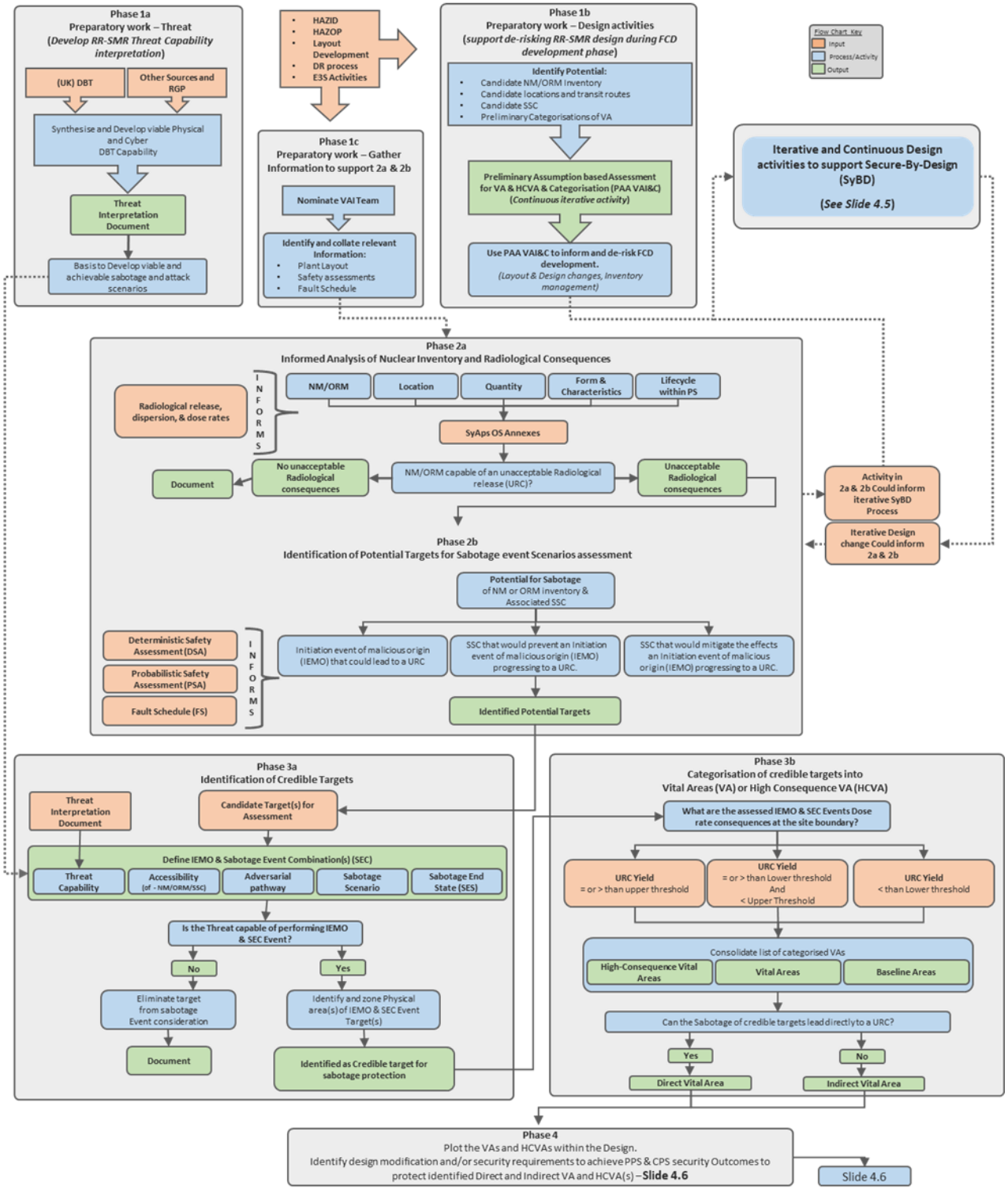


Figure 32.10-1 – Initial Vital Area Identification and Categorisation Methodology

32.10.3 Phase 1 – Preparatory Work

To show concurrent activity to prepare for the assessment.

Phase 1a –Threat –

Taken from the Threat Interpretation.

Phase 1b – Design Activities

The initial application of PAA to continue to de-risk the design of the RR SMR.

Phase 1c – Information Gathering

To gather the team, Subject Matter Experts and documentation to support the assessment.

32.10.4 Phase 2 – Analysis of Nuclear Inventory and Identification of Potential Targets

Phase 2a – Informed Analysis of Nuclear Inventory and Radiological Consequences

To identify the NM/ORM inventory for the RR SMR and to determine from the quantity and type of material found at each location whether its sabotage would or would not likely cause a URC.

Phase 2b – Identification of Potential Targets for Sabotage Event Scenarios

To identify the Initiating Event of Malicious Origin (IEMO) that could cause a URC and the SSCs that would also need to be compromised to enable the event to progress to a URC. These are identified as Potential Targets within a Potential Sabotage Event Scenario (PSES).

32.10.5 Phase 3 – Identify Credible Targets and Categorise Vital Areas

Phase 3a – Identification of Credible Targets

The Threat Capability from the Threat Interpretation is applied to determine whether the adversary force has the capability to commit the IEMO and compromise the PSES. Where this is possible, the PSES becomes a Sabotage Event Scenario (SES) and Potential Targets become Targets. Cyber, physical and blended attack methods are considered in this sub-phase.

Phase 3b – Categorisation of Credible Targets into Vital Areas

The dose rates from each credible IEMO and SES Event are categorised and the targets are located within VAs or HCVAs depending on each URC consequence. These areas are further identified as Direct or Indirect, depending on whether the IEMO will lead directly to a URC or whether an SES Event also needs to be compromised to reach the same outcome.

32.10.6 Phase 4 – Vital Area Locations within the Rolls-Royce SMR

Design modifications are considered to reduce the consequence of Vital Areas or remove them altogether, and security measures are designed in to deliver the required levels to achieve the Physical Protection System (PPS) SORPs.

Phase 4 of the Methodology requires the interaction between the Security Case Team and the Engineering Design Team to design out vulnerabilities and then to design in security measures where required. This phase is shown in more detail in Figure 32.10-2.

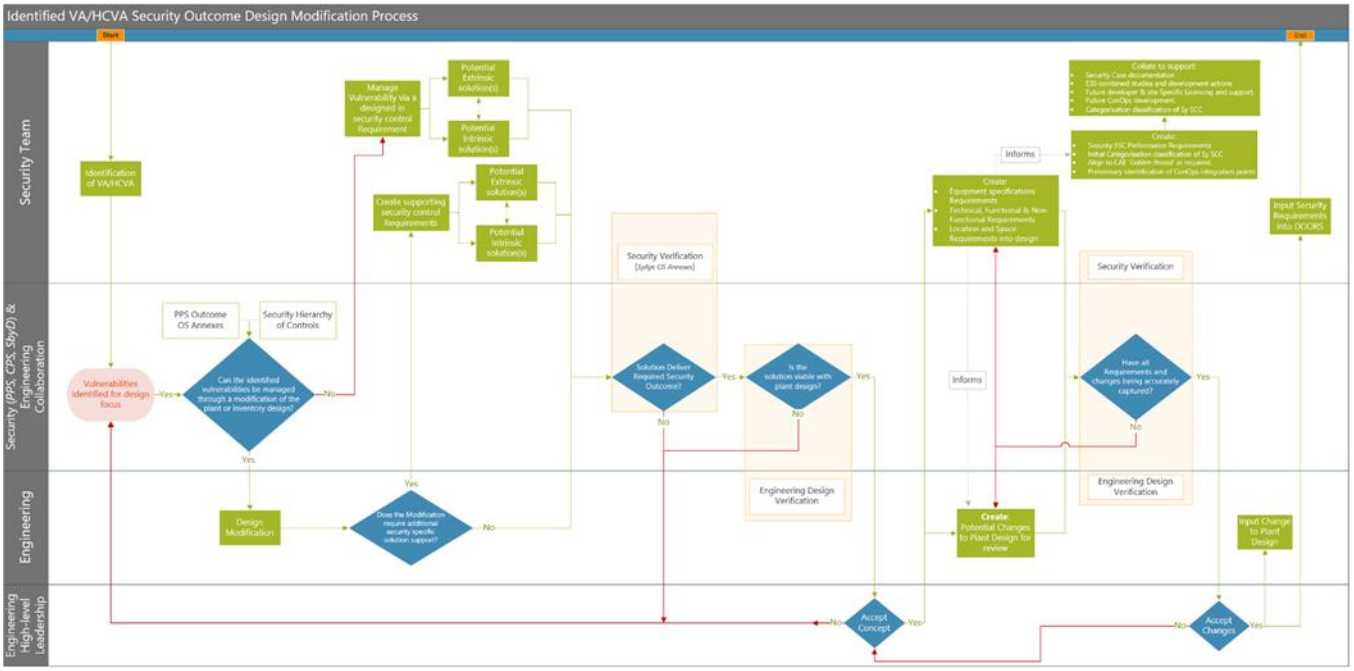


Figure 32.10-2 – Vital Area Identification and Categorisation Methodology – Phase 4

32.10.7 Output from Vital Area Identification and Categorisation

The output from the Vital Area Identification and Categorisation assessment is a list of categorised Vital Areas, their locations and potential security measures to design into the engineering design that will achieve the PPS SORPs. Cyber-attack vectors and blended attacks are also considered as part of this assessment.

32.11 Secure by Design

32.11.1 Introduction

Secure by Design (SbyD) is a KSyPP from SyAPs (Reference [2]), and the Security Case must demonstrate how it has been applied to the maturing design. It must also provide evidence that the RR SMR will comprise an inherently secure design that is consistent with its operation and where security has been considered from the initial design stage.

The Hierarchy of Security Controls that should be considered when applying the SbyD Principle have been taken from SyAPs (Reference [2]) and are shown in Figure 32.11-1.

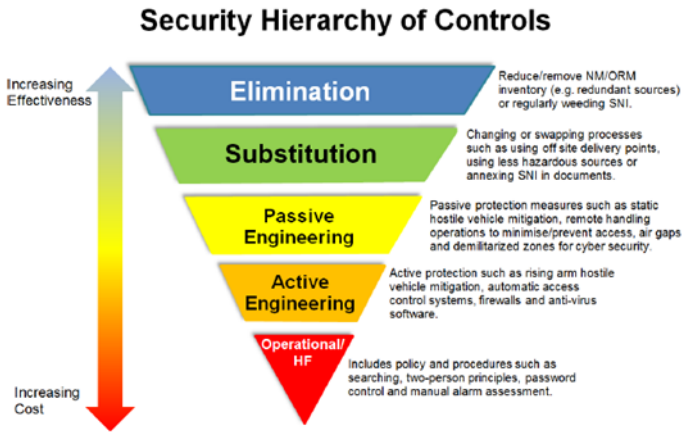


Figure 32.11-1 – Security Hierarchy of Controls

The RR SMR offers a unique opportunity to apply the SbyD Principle as a nuclear power plant is being designed in parallel with the development of the E3S Case. This has enabled the Security Case Team to work in tandem with the Design Engineers to identify security vulnerabilities and to offer solutions to design them out.

The SbyD methodology is currently under development, but its principle is being applied to the design currently, and evidence is being gathered. This section will describe the methodology, its application and provide evidence of the outcomes.

This section is envisaged to comprise the sub-sections outlined below.

32.11.2 Claims Addressed

This Sub-section will set out the Top Level Claims and Sub-Claims that are to be substantiated by this Section.

32.11.3 Principles

A preliminary set of Security Principles and Security by Design Principles were set out in the PSyR (Reference [1]). These principles have been communicated to engineers to assist them

with designing a power station that is, as far as is reasonably practicable, inherently secure and consistent with operational purposes.

The application of these principles is monitored through the integrated design activities, design decisions and change control.

These principles may be further developed as the RR SMR (and GSR) matures.

32.11.4 Requirements

Overarching security requirements are entered into the power station requirements at the top level of the requirements structure and allocated to the PPS, CPS and non-security SSCs delivering security functions, for example, buildings, containment and landscaping.

Figure 32.11-2 shows the flow of requirements from the power station level down to the SSCs, both direct and via the design of an integrated site security system, PPS and CPS. Blue boxes indicate general (both functional and non-functional) requirements, green boxes indicate non-functional requirements, and red boxes indicate functional requirements. The majority of requirements relating to secure by design will be communicated as non-functional requirements.

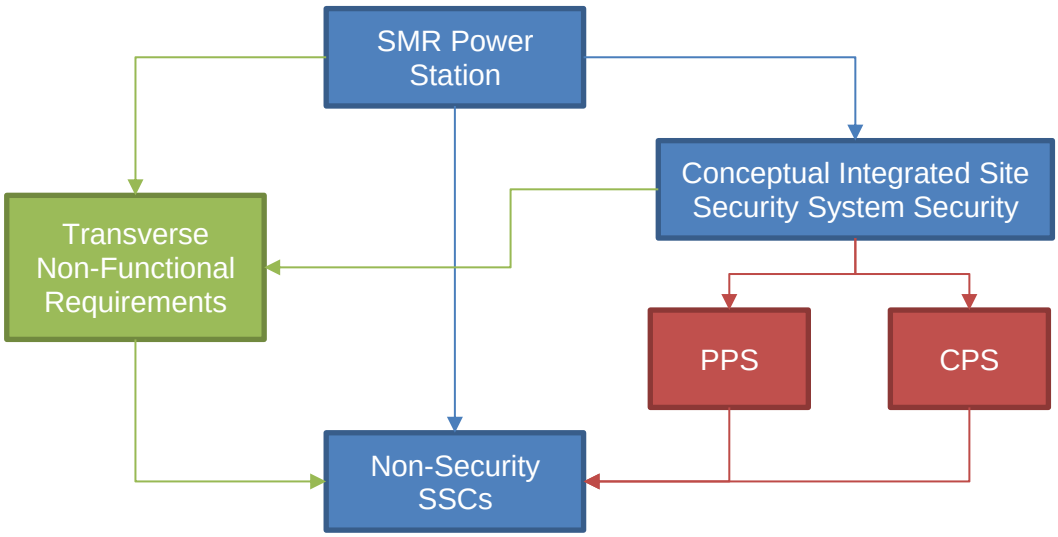


Figure 32.11-2 - Flow of Security Requirements

The allocation for security functional requirements against non-SSCs ensures that the security functions being delivered by these SSCs are adequately captured in the design and reviewed whenever changes are proposed.

32.11.5 Codes and Standards

Adherence to appropriate cyber security standards, such as BS EN IEC 62645, has the potential to significantly reduce the inherent cyber security risk in Control and Instrumentation (C&I) systems and other Operational Technology (OT), as these standards ensure that the resultant systems are architected in a way that enhances their defensibility against cyber security threats.

Codes are available for the design of the built environment to control or mitigate the risk from blast and hostile vehicles; these will also be used in the design of architectural features to minimise inherent physical security risk.

32.11.6 Integrated Design Activities

Security is an active stakeholder in most of the major SSCs that form the RR SMR.

This includes for example: Hazard and Operability studies, Hazard Identification studies, and architecture studies).

32.11.7 Design Decisions

This includes for example: Gate Reviews, Design Reviews, Decision Records.

32.11.8 Iterative Design

To re-evaluate designs when risk levels exceed risk appetites.

32.11.9 Change Control

This sub-section will summarise the change control process that will be adopted and reference out to more detail.

32.11.10 Validation and Verification

This sub-section will address the validation and verification that will be undertaken as part of the approach to SbyD.

32.12 Integration with Other Topic Areas

32.12.1 Introduction

The GSR is an integrated chapter within the E3S Case and the security assessment will not be conducted in isolation. There will be considerable interaction with other Topic Areas described in further chapters.

The Topic Areas (chapters in the E3S) that the GSR will be integrated with will include (but not necessarily be limited to) those shown in Table 32.12-1.

Table 32.12-1: E3S Case Chapters Integrating with GSR

No.	Title	Summary of Contents
1	Introduction	Presents the approach to and structure of the integrated E3S Case
3	E3S Objectives & Design Rules for Structures, Systems & Components	Presents the key principles and associated methods, approaches, and requirements that provide the framework for the RR SMR to achieve its E3S objectives
4	Reactor (Fuel & Core)	Describes the fuel and core design, including its composition and configuration of fuel, control rods, etc., and associated operational parameters
5	Reactor Coolant System & Associated Systems	Describes the Reactor Coolant System (RCS) and associated systems, which include the Reactor Pressure Vessel (RPV) and the primary coolant circuit components
6	Engineered Safety Features	Describes the systems which deliver the safety functions in response to fault and accident conditions in the reactor
7	Instrumentation & Control	Describes the Control & Instrumentation (C&I) systems which support delivery of the safety functions
8	Electrical Power	Describes the electrical power systems which supply power to systems during both normal and fault conditions
9A	Auxiliary Systems	Describes the auxiliary systems of the RR SMR, including the fuel handling and storage systems, water supply systems, and ventilation systems
9B	Civil Engineering Works and Structures	Describes the civil and structural design aspects of the RR SMR, including the hazard shield and the base isolation system for protection against external hazards
11	Management of Radioactive Waste	Describes the radioactive waste treatment systems for RR SMR, and summarises the sources of solid, liquid, and gaseous waste streams as well as the anticipated quantities, arrangements for waste minimisation, and disposal routes

No.	Title	Summary of Contents
12	Radiation Protection	Evaluates how radiation doses to onsite workers and members of the public will be controlled during normal operations, and describes the design features of the RR SMR that minimise exposures to ALARP
13	Conduct of Operations	Presents how the RR SMR fulfils its prime responsibility for the safety in operation, including organisational arrangements, competencies and training programmes, operational safety programmes, and operating procedures and guidelines
15	Safety Analysis	Presents the methods and outputs of the safety analysis that evaluate the RR SMR against relevant criteria and inform the design development, including the deterministic analysis of faults and accidents, probabilistic analysis, and internal and external hazard assessment
16	Operational Limits & Conditions	Presents the processes to define the Operational Limits & Conditions (OLCs) in the design and safety analysis, to ensure they are successfully transferred into operational documentation
18	Human Factors Engineering	Provides the demonstration that Human Factors (HF) is fully integrated into the RR SMR and substantiation processes
22	Conventional & Fire Safety	Presents the strategies for implementation of conventional and fire safety into design of the RR SMR, including Construction Design and Management (CDM)
23	Structural Integrity	Presents the demonstration of structural integrity for safety-classified metallic pressure boundary components and their supports
25	Detailed information about the design	Presents a technical description of the facility's main plants, systems and processes, which have a bearing on radioactive waste (solid, liquid and gaseous) generation, treatment, measurement, assessment and disposal, drawing upon information from other E3S Case chapters
26	Detailed description of radioactive waste management arrangements	Presents the Radioactive Waste Management Arrangements (RWMA) for RR SMR, including an overview of waste minimisation with focus on disposability and optimised disposal routes
33	Safeguards	Presents the demonstration that the RR SMR facilitates Safeguards through material accountability, and containment and surveillance

32.13 Security Categorisation and Classification

32.13.1 Introduction

The security functional categorisation and classification of systems is covered by KSyPP 5 from SyAPs (Reference [2]) and is used to ensure the reliability and capability of a site's security measures.

The GSR will demonstrate how KSyPP 5 has been applied from the following definitions:

1. Security Functional Categorisation – the security functions to be delivered should be identified and categorised, based on their significance regarding security

2. Security Functional Classification – SSCs that must deliver security functions should be identified and classified on the basis of those functions and their significance to security.

This section will describe the methodology that Rolls-Royce SMR has developed to apply the KSyPP and the outcomes of its assessment.

32.13.2 Claims Addressed

This sub-section will set out the Top Level Claims and Sub-Claims that are to be substantiated by this Section.

32.14 Conceptual Integrated Security Solution

32.14.1 Introduction

Previous sections within the GSR have identified:

1. Locations containing NM/ORM that requires protection from theft
2. Vital Areas that require protection from sabotage
3. The OT, CBSIS and CBSy that need protection from sabotage
4. The SORPs for PPS and CPS to achieve based on the categorisation of material from theft or the consequence of the loss of a system.

This section will draw this information together and propose a Conceptual Integrated Security Solution (CISS) that will combine physical and cyber measures to deliver the appropriate levels of protection that will be required across the site. The solution will adopt the philosophy of 'inside to outside security', which means the security system will start with the target that needs protection and apply layers until it reaches the outer boundary of the site.

There will be a further integration exercise to ensure that the CISS does not impede plant operations and safety measures.

The security solution will also apply the following KSyPPs:

1. **KSyPP 3, The Graded Approach** – Protection systems should be based on a graded approach, taking into account the categorisation for theft or sabotage of NM/ORM
2. **KSyPP 4, Defence in Depth** – Protection systems should reflect a concept of several layers and methods of protection that have to be overcome or circumvented by an adversary and ensure appropriate mitigation of security events should prevention fail.

The level of detail that will be provided within the CISS will be defined but it will be presented at a level that will be beneficial to a future SL.

The codes and standards for the identified security measures used within the CISS will be presented to support the future SL. KSyPP 7 (Reference [1]) outlines the regulatory expectation regarding codes and standards.

32.14.2 Claims Addressed

This sub-section will set out the Top Level Claims and Sub-Claims that are to be substantiated by this Section.

32.15 Concept of Security Operations

32.15.1 Introduction

The Security Case should include a high-level Concept of Operations that will describe how the CISS will operate. This section will demonstrate:

1. How PPS and CPS measures will be successfully integrated

2. That a proportionate 'due diligence' approach has been adopted to provide sufficient power, back-up power, room and space, in-built security measures and ventilation systems to support a reasonably foreseeable security system

3. How the functional categorisation and classification of SSCs delivering security functions will be supported through an Examination, Maintenance, Inspection and Testing regime

4. The priority for the restoration of security systems to deliver security functions.

32.15.2 Claims Addressed

This sub-section will set out the Top Level Claims and Sub-Claims that are to be substantiated by this Section.

32.16 Development of GSR to a Security Plan for Site Licensee

32.16.1 Introduction

The GSR will form the basis of the NSSP that will be prepared by the future SL in line with SyAPs (Reference [2]) for assessment by the ONR. The CISS will then be developed into a detailed, site-based design. This section will describe how the GSR will:

1. Expand to form the foundation of the NSSP
2. Transfer knowledge and arrangements to the future SL to put into practice
3. Provide evidence that the GSR will be suitable for implementation as part of an operating regime.

32.17 Assumptions, Commitments and Requirements

32.17.1 Introduction

The capture of assumptions, commitments and requirements is essential to support the future SL in developing and implementing an effective, site-specific NSSP. It is also vital to support the knowledge transfer to explain the principles behind the decisions taken within the GSR and to describe what the future SL must develop in the NSSP.

This section is envisaged to include the sub-sections outlined below.

32.17.2 Assumptions

To explain the bases on which certain decisions were made and to describe features that would form part of the case to meet security outcomes.

32.17.3 Commitments

To describe obligations that have been placed on the future SL to deliver in order to meet security outcomes.

32.17.4 Requirements (for future Site Licensee)

To describe the requirements and standards that solutions must achieve to deliver the security functions and meet security outcomes.

Although these requirements and standards will form part of the RR SMR design, their delivery and implementation will be the responsibility of the future SL.

32.18 Conclusion

32.18.1 Introduction

This section will complete the report and summarise its findings to demonstrate that the security claims have been met and that the RR SMR may be operated in a way that will protect the public from the effects of theft or sabotage of NM/ORM.

32.19 References

[1] Rolls-Royce SMR, SMR0001610, Issue1, " Rolls-Royce Small Modular Reactor (RR SMR) - Preliminary Security Report," August 2022.

[2] Office for Nuclear Regulation, "Security Assessment Principles for the Civil Nuclear Industry (Version1)," March 2022.

[3] "Nuclear Security Industries Regulations, 2003, SI 2003:no. 403".

[4] Rolls-Royce SMR, SMR 0002183, Issue 2, "Rolls-Royce SMR Generic Design Assessment Scope," January 2023.

[5] Rolls-Royce, SMR0000594, Issue 1, "RR SMR Design Overview Report," June 2022.

32.20 Acronyms and Abbreviations

ASCE	Assurance and Safety Case Environment
CAE	Claims, Arguments and Evidence
CBSIS	Computer Based Systems Important to (Nuclear) Safety
CBSy	Computer Based Security
CDM	Construction Design and Management
C&I	Control & Instrumentation
CISS	Conceptual Integrated Security Solution
CPS	Cyber Protection System
CSRA	Cyber Security Risk Assessment
DBT	Design Basis Threat
E3S	Environment, Safety, Security and Safeguards
FSyP	Fundamental Security Principle
GDA	Generic Design Assessment
GSR	Generic Security Report
HCVA	High Consequence Vital Area
HF	Human Factors
IEMO	Initiating Event of Malicious Origin
KSyPP	Key Security Plan Principle
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations 2003
NM	Nuclear Material
NSSP	Nuclear Site Security Plan
OLC	Operating Limits and Conditions

ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
PAA	Preliminary Assumption-Based Assessment
PPS	Physical Protection System
PSES	Potential Sabotage Event Scenario
PSyR	Preliminary Security Report
RGP	Relevant Good Practice
RR SMR	Rolls-Royce Small Modular Reactor (the design)
RCS	Reactor Coolant System
RPV	Reactor Pressure Vessel
RWMA	Radioactive Waste management Arrangements
SbyD	Secure by Design
SES	Sabotage Event Scenario
SL	Site Licensee
SORP	Security Outcome, Response and Posture
SSC	Structure, System or Component
SyAPs	Security Assessment Principles
URC	Unacceptable Radiological Consequence
VA	Vital Area