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

Title

Rolls-Royce Small Modular Reactor (RR SMR) - Preliminary Security Report (PSyR)

Executive Summary

This document is the Preliminary Security Report (PSyR) for the RR SMR.

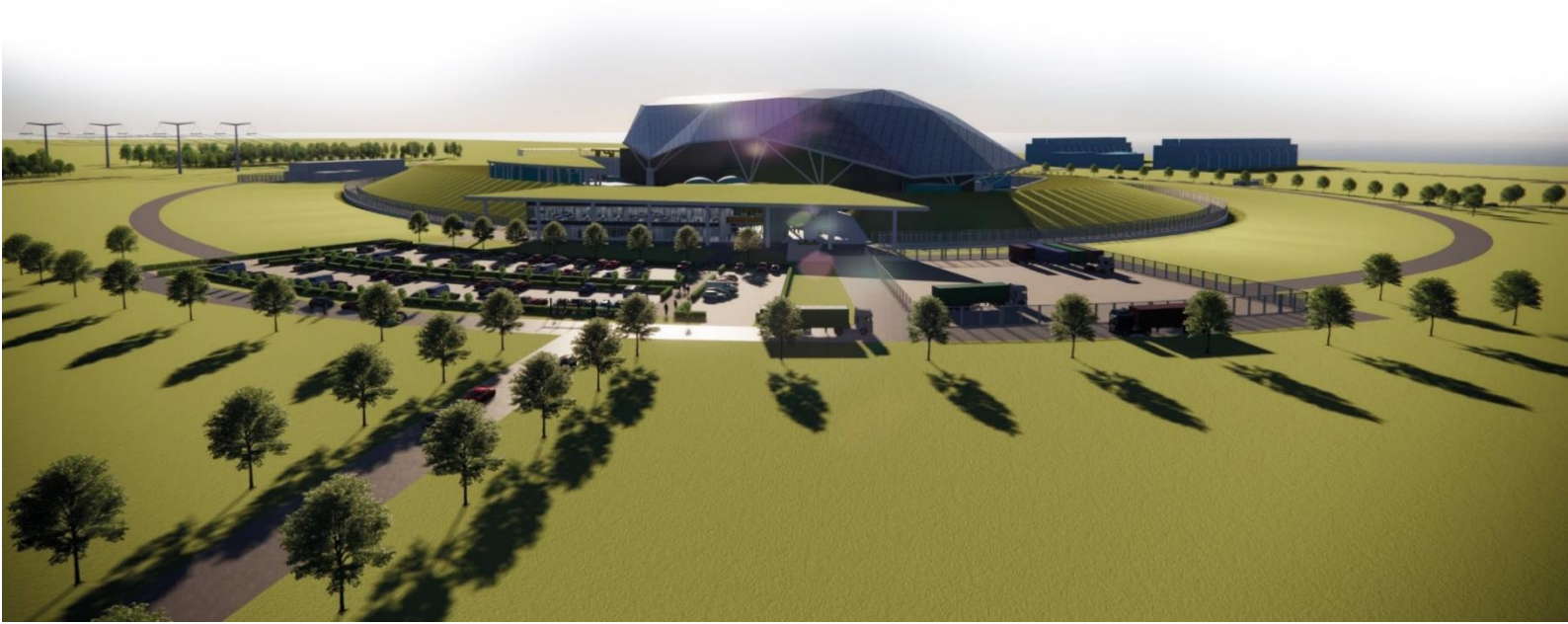
This PSyR sets out the Security Objectives and Design Principles that will drive a systems engineering approach to the development of the security arrangements for the RR SMR. These arrangements will be substantiated within a subsequent Generic Security Report (GSR), which will be structured using a 'claims-argument-evidence' approach.

The PSyR provides a baseline for the subsequent development of the GSR and supporting documents. The higher-level security claims that will form the backbone of the GSR will address:

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

The philosophy behind the PSyR (and subsequent GSR) is a risk-informed approach to design, which recognises the need to provide a 'graded approach' to the provision of protection against the potential for harm to people and the environment. As emphasised throughout this PSyR, the commitment to build security into the RR SMR engineering design has been in-place from the start of the RR SMR design programme and, security professionals have provided advice and input from the concept design phase onwards.

The PSyR is a 'one-off' document and will not be up-issued as the design of the security arrangements matures.



Contents

1 Introduction

1.1 Objective of the PSyR

1.1.1 This document is the Preliminary Security Report (PSyR) for the Rolls-Royce Small Modular Reactor design (the RR SMR). The objective of the PSyR is to provide a high-level overview of the basis on which the nuclear security arrangements for the RR SMR will be developed.

1.1.2 These security arrangements will be developed (in the first instance) on the basis of the requirements of UK civil nuclear law, and of relevant guidance and good practice. The construction and operation of a RR SMR outside of the UK will require a review of the applicable regulatory regime for that location.

1.1.3 This PSyR does not present these security arrangements nor seek to substantiate such. The development and substantiation of the security arrangements will be set out in a Generic Security Report (GSR).

1.1.4 The GSR will represent the Security Case for the generic RR SMR. Subsequent construction and operation of a RR SMR will require further development of a site-specific Security Case and ultimately (in the UK) of Nuclear Site Security Plan (NSSP).

1.1.5 In accordance with accepted good practice, the GSR will be presented in a 'claims-argument-evidence' approach. The GSR will be supported by appropriate topic reports and other evidential documents.

1.1.6 The philosophy behind the PSyR (and subsequent GSR) is a risk informed approach to design, which recognises the need to provide a 'graded approach' to the provision of protection against the potential for harm to people and the environment, should malicious acts lead to an Unacceptable Radiological Consequence (URC).

1.1.7 This PSyR seeks:

1. To indicate how the requirements of UK regulatory regime for nuclear security and relevant good practice will inform the security arrangements for the RR SMR.

2. To present the top-level nuclear security claims that form the basis of the risk informed nuclear security arrangements; the PSyR does not present any substantiation of these claims

3. To outline proposals for the development of the subsequent GSR.

1.1.8 Rolls-Royce SMR has chosen to submit the design of the RR SMR to a Generic Design Assessment (GDA). This GDA will run alongside the maturing design; the correspondence between design maturities and the stages (steps) of the GDA is outlined in paragraph 1.3.3.

1.2 Generic Design Assessment

1.2.1 This PSyR will be submitted to the Office for Nuclear Regulation (ONR) during Step 1 of the GDA for the RR-SMR, to provide a basis for initial discussions on nuclear security topics between Rolls-Royce SMR (as Requesting Party) and the ONR at GDA Step 1.

1.2.2 Rolls-Royce SMR understands the objective for GDA is to provide confidence that the proposed design is capable of being constructed, operated and decommissioned in the UK in accordance with the relevant standards of safety, security and environmental protection.

1.2.3 The GDA process has three steps, which can be summarised as:

Step 1 – Initiation

Step 2 – Fundamental Assessment

Step 3 – Detailed Assessment.

1.2.4 Rolls-Royce SMR recognises that the ONR is responsible for the assessment of the nuclear safety and security submissions. Rolls-Royce SMR is familiar with the expectations of the ONR presented within in their guidance to RPs (Reference [1]) and in the ONR Security Assessment Principles (SyAPs) (Reference [2]).

1.3 Rolls-Royce SMR

Definitions

1.3.1 For a point of clarity, the following terms which are used throughout this document are defined as:

1. **Rolls-Royce SMR** – is the corporate entity which is undertaking the design of the small modular reactor and is the Requesting Party for the GDA.

2. **RR SMR** – is the design of the new power station which is being submitted for assessment.

RR SMR Reference Design

1.3.2 The increasing maturity of design for the RR SMR is controlled through a gated Definition Review (DR) process. This is the key technical control process to ensure that the design definition is delivered in line with specified requirements. Prior to entry into GDA, the design maturity was progressing from Phase 1 to Phase 2 of a Preliminary Concept Design (PCD). Further detail of the DR process is provided in the Rolls-Royce SMR Engineering Management Plan (Reference [3]).

1.3.3 Currently, it is understood that the following design maturities will be defined as Design Reference Points as the RR-SMR progresses through GDA:

1. GDA Step 1 – Preliminary Concept Definition Phase 2 (PCD2)

2. GDA Step 2 – Full Concept Definition (FCD)

3. GDA Step 3 – Developed Design (DD)

1.3.4 The intention is that design maturity coincident with end of GDA Step 3 would define the Design Reference Point for a subsequent site-specific Nuclear Site Licence (NSL) application and the development of the GSR (Final) into a NSSP.

Stakeholders (Engineering)

1.3.5 RR SMR is a complex, multi-disciplinary design and engineering project. The project is adopting a 'secure by design' approach, whereby nuclear security is integrated into the overall engineering design.

1.3.6 This integrated approach to security (which is outlined in this PSyR) involves a variety of engineering and other disciplines; all of which contribute to delivery of the security arrangements for the RR SMR

1.3.7 Key interfaces are with: safety case engineers, nuclear island design engineers and civil engineers (in terms of physical protection); and Operational Technology (OT) / Information Technology (IT) engineers (in terms of cyber security). Not all stakeholders will be involved in all aspects of the security arrangements for the RR SMR.

Environment, Safety, Security and Safeguards (E3S)

1.3.8 One of the fundamental objectives of the design of the RR SMR is…

'…to protect people and the environment from harm'

1.3.9 The achievement of this fundamental objective will be demonstrated through substantiation of the RR SMR against principles and claims covering nuclear safety, environmental protection, nuclear security and safeguards. This will be documented within the following:

1. A Nuclear Safety Case
2. An Environmental (Protection) Case
3. A Nuclear Security Case
4. Nuclear Safeguards Case.

1.3.10 These 'cases' are being developed using an integrated and co-ordinated approach within Rolls-Royce SMR; and are colloquially referred to as the 'E3S Case'. This approach is outlined further in Section 4.

1.3.11 The systems engineering approach to the RR SMR design development outlined in Engineering Management Plan, Reference [3], includes E3S as key stakeholders in the DR process.

GDA Boundary

1.3.12 The boundary of GDA assessment for the RR SMR remains to be finalised.

1.3.13 An initial list of Structures, Systems and Components (SSCs) to be included was set out prior to GDA entry in the SMR Generic Design Assessment Boundary Document (Reference [4]); but with an acknowledgement that this list was subject to revision as the design matured further.

1.3.14 This initial list was based around the inclusion of SSCs which were important to:

1. Nuclear Safety
2. Protection of the Environment
3. Nuclear Security.

1.3.15 The nuclear safety case identifies postulated initiating events (PIEs) which, if not protected against, can result in a radiological consequence. Any SSCs that are required to protect or mitigate against these PIEs, or whose failure could cause a PIE, are to be included in the GDA boundary. From a security perspective, some of these PIEs could be caused by a malicious act. This combined with the deliberate disabling of protective/mitigating SSCs could lead to an Unacceptable Radiological Consequence (URC). Therefore, if an SSC is included in the GDA boundary for nuclear safety then it is also assumed that it is important from a security point of view

1.3.16 The GDA Boundary document (Reference [4]) did not consider operational states or lifecycle phase. Those to be included in the assessment (and, therefore, considered with regard to nuclear security) require agreement between the ONR and Rolls-Royce SMR.

1.3.17 A summary introduction to the SMR design is presented in Sub-Section 7.1.11.

1.4 Structure of the PSyR

1.4.1 The structure of this PSyR is as follows:

Section 1, Introduction – This section introduces the PSyR, its purpose, contents and structure.

Section 2, Nuclear Security, **Regulation and Guidance** – This section outlines the regulatory requirements and sources of guidance and relevant good practice that inform the development of the security arrangements for the RR SMR.

Section 3, Generic Security Report – This section outlines the proposed development of the GSR as the design matures and the GDA progresses.

Section 4, Development of the E3S Case – This section introduces the fundamental E3S principle and provides an overview of the integrated approach to an overall E3S Case and the common 'claims-argument-evidence' approach that will be adopted in the cases for the individual disciplines.

Section 5, Security Objectives and Principals – This section sets out the security objectives for RR SMR and outlines the design principles and security functions that will be adopted to deliver these objectives. The integration of nuclear safety into engineering design and nuclear safety is also discussed.

Section 6, Nuclear Security Claims – This section introduces the Fundamental and Tier 1 nuclear security claims. The Tier 1 claims cover: the Security Design Basis; Protection from Sabotage; Protection from Theft; and Cyber Security & Information Assurance. This section also outlines how lower-level claims will be developed and the overall 'claims -arguments-evidence' architecture that will be adopted in the GSR. (*Subsequent Sections 7, 8 and 9 outline the basis on which these claims will be justified and substantiated*.)

Section 7, Security Design Basis – This section outlines the security design basis for the RR SMR. The topics covered include: Secure by Design Principles, Threat Assessment and Vulnerability Assessment.

Section 8, Physical Protection Solution – This section outlines the approach that will be taken for the design of a Physical Protection System (PPS) for the RR SMR; this covers target identification for sabotage and theft, the identification of the required security outcomes and the possible use of an Operational Requirements process to deliver these outcomes.

Section 9, Cyber Security & Information Assurance – This section outlines the approach that will be taken in the design of Cyber Security and Information Assurance (CS&IA) arrangements for the RR SMR; this covers the scope of CS&IA and its implications for OT and IT.

Section 10, Summary and Integration with Engineering Design – This Section sets out a high-level summary of the PSyR and our proposed approach to development of the GSR, together with outline details of how security has interfaced with and integrated into engineering design (prior to the start of GDA).

1.5 Limitations and Exclusions

Limitations

1.5.1 This document was crafted to reflect programme information available at the time of publication. Programme development continues unabated, and future iterations of the GSR will capture changes.

1.5.2 This PSyR has been written on the basis that the boundary (scope) of the GDA has yet to be finalised, as set out in Paragraph 1.3.12. Notwithstanding this agreement, the proposed scope of the GSR will address primarily the operating phase of a nuclear power station. It is proposed that the GSR will not cover security during manufacture, construction or commissioning lifecycle phases.

1.5.3 This PSyR assumes that we are developing the security arrangements necessary to protect a single operational RR SMR unit. The possible implication of sharing security arrangement across co-located multiple units or across a fleet of locations will be considered, as necessary, within the GSR.

1.5.4 This PSyR assumes that the generic RR SMR site is not located adjacent to other nuclear licensed facilities. On this basis, the GSR will not consider security arrangements associated with the RR SMR design being adjacent to (or an enclave in) an existing nuclear licensed site. This would be addressed in a subsequent site specific security case.

Exclusions

1.5.5 This PSyR does not cover the topic of Safeguards. Safeguards will be addressed, as appropriate, within a separate generic safeguards report.

1.5.6 This PSyR does not consider the topic of security during the off-site transport of regulated nuclear material. Nor is it proposed that such will be considered within any subsequent GSR. This is a topic which is considered to be outside the scope of the security assessment at GDA.

1.6 Classification Statement for this Document

1.6.1 None of the information contained within this PSyR is considered to be Sensitive Nuclear Information (SNI), as defined in accordance with the ONR Classification Policy for the Civil Nuclear Industry (Reference [5]).

2 Nuclear Security – UK Regulation & Guidance

2.1 Introduction

2.1.1 This section of the PSyR summarises the International and UK regulation and associated guidance documents which inform the requirements and expectations for the RR SMR security.

2.1.2 In particular, the sources referenced in this section have informed the derivation of our security objective and principles (see Section 5), our high-level security claims. (see Sub-section 6.2) and our secure by design principles (see Sub-section 7.3).

2.2 International Regulation and Guidance

2.2.1 The UK is obliged to establish and maintain a legislative framework to govern the physical protection of Nuclear Material (NM), Other Radioactive Materials (ORM) and Sensitive Nuclear Information (SNI) in accordance with the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference [6]) The CPPNM and Amendment (Reference [7]) places obligations on signatory states to protect nuclear facilities, and material in peaceful domestic use, in storage and in transit.

2.2.2 The UK is also a signatory to the United Nations International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT); which requires signatories to make every effort to adopt appropriate measures to ensure the protection of radioactive material.

2.2.3 Both these conventions refer to the functions of the International Atomic Energy Agency (IAEA) and the guidance which it provides.

2.2.4 With regard to nuclear security matters and the objectives of this PSyR, relevant IAEA Guidance includes:

1. Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control IAEA, Nuclear Security Series No 34-T, 2019 (Reference [8]).

2. Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), Implementing Guide No. 27-G, 2018 (Reference [9]).

3. Identification of Vital Areas at Nuclear Facilities, Technical Guidance Reference Manual, Technical Guidance No. 16, 2013 (Reference [10]).

2.3 UK Regulation

2.3.1 The principal UK legislation which regulates the Civil Nuclear Industry in the UK is summarised below.

Nuclear Installations Act 1965

2.3.2 Under the Nuclear Installations Act 1965 (NIA), the construction and operation of a nuclear power station (in the UK) will require a Nuclear Site Licence (NSL). An NSL can only be granted to a corporate body/organisation. Once granted, the NSL cannot be transferred and is applicable only to the specific site for which it was granted.

2.3.3 The NSL covers the entire lifecycle of a nuclear site from installation and commissioning through operation and decommissioning to site clearance and remediation.

2.3.4 The three key themes that ONR will addresses as part of a licence application are:

1. The capability, organisation and resources of the applicant corporate body.
2. The nature of the prescribed activities and the relevant safety case(s).
3. The nature and location of the site.

Nuclear Industries Security Regulations 2003 (NISR)

2.3.5 The NISR 2003 (as amended) place significant obligations on the operators of civil licensed nuclear sites relating to physical security measures for facilities, nuclear material and the security of SNI. This legislation requires all civil nuclear operators to produce and implement robust Nuclear Site Security Plans (NSSPs).

2.3.6 During a GDA, NISR is only applicable to a Requesting Party with regard to the protection of SNI. However, the Requesting Party must demonstrate that the GDA design is capable of operation (etc.) in full compliance with NISR.

2.4 ONR Guidance

2.4.1 The ONR was established as a statutory Public Corporation on 1 April 2014 under the Energy Act 2013 and is the principal independent regulator for nuclear safety and security in UK Civil Nuclear industry.

2.4.2 Within the ONR, ONR Civil Nuclear Security and Safeguards (ONR CNSS) is responsible for the implementation of UK legalisation covering nuclear security.

2.4.3 ONR produce a range of guidance documents with regard to nuclear security in the UK civil nuclear industry. A brief summary of the main relevant guidance is provided below.

2.4.4 In part, the ONR guidance is written to aid the ONR in the execution of its assessment and other regulatory duties. Nevertheless, this guidance, when taken together, sets out the expectations of the ONR with regard to nuclear security.

2.4.5 In developing their guidance, the ONR have taken into account international good practice set out in IAEA recommendations and guidance.

2.4.6 The primary purpose of the Security Assessment Principles (SyAPs) is to provide ONR with a framework for making consistent regulatory judgements on the adequacy of

security arrangements. The principles are supported by Technical Assessment Guides (TAGs), Technical Inspection Guides (TIGs) and other guidance, to further assist decision making within their nuclear security regulatory assessment processes.

Security Assessment Principles

2.4.7 The SyAPs (Reference [2]) provide guidance to Dutyholders (NSL holders and others subject to regulation by the ONR) on the expectations of the ONR for nuclear security. The SyAPs represent ONR's view of good practice and ONR expect modern facilities to satisfy their overall intent.

2.4.8 The SyAPs replace the previously prescriptive approach to regulation of Nuclear Security with an 'outcome focussed' approach whilst also transferring responsibility for risk ownership to the Dutyholder. This is similar to the ONR's approach to the regulation of nuclear safety which utilises the ONR Safety Assessment Principles (SAPs) (Reference [11]).

2.4.9 This outcome-based approach to regulation provides a framework for the consistent application of the principles advocated by the IAEA to ensure proportionality through application of the graded approach, the principle of secure by design, defence in depth; and address the requirements of key international obligations.

2.4.10 The SyAPs are presented in four sets:

1. **Fundamental Security Principles (FSyP)** – these are principles which underpin all the activities that contribute to a sustained high standard of nuclear security. The FSyPs fall into two categories:

   a. 'Strategic Enablers' (FSyP 1 to 5), which are focused on the creation of the right conditions to support high reliability security arrangements (i.e. they are concerned with enabling the delivery of an effective security strategy).

   b. 'Secure Operations' (FSyP 6 to 10), which are focused on the implementation and maintenance of nuclear security (i.e. they are concerned with the delivery of secure operations).

2. **Security Delivery Principles (SyDP)** – these support the Fundamental Security Principles and set out the specific outcomes that will deliver an effective nuclear security regime.

3. **Key Security Plan Principles (KSyPP)** – these are principles which can be applied across the breadth of the FSyPs and SyDPs.

4. **Regulatory Assessment of Security Plans (RASyP)** – these are principles which set out the foundations for effective security plans.

2.4.11 The majority of the FSyPs and SyDPs which cover 'Strategic Enablers' are relevant to a Requesting Party submitting a reactor design into the GDA process; and, would be expected to be addressed within a demonstration that the Requesting Party is a 'competent' organisation, rather than within a PSyR or GSR.

2.4.12 The relevance and applicability of the individual SyAPs to a GDA nuclear security submission is discussed (at a high-level) within this PSyR and will be further discussed within the subsequent GSR iterations, which will be based around demonstrating compliance to the relevant SyAPs.

2.4.13 The SyAPs are accompanied by a series of Annexes which outline a series of 'postures' and 'outcomes' to inform the requirements for a physical protection System (PPS) and cyber security and information assurance (CS&IA).

2.4.14 The SyAPs annexes are classified at Official-Sensitive: SNI. No significant reference has been made to these annexes in the drafting of this PSyR. The annexes will be consulted during the subsequent further development of the GDA nuclear security submission; and will play an important part in our Secure by Design approach.

GDA Specific Guidance

2.4.15 The ONR has issued guidance on how it will undertake a GDA assessment process and its expectations of Requesting Parties. This guidance is as follows:

1. New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-006, Revision 0, October 2019 (Reference [1]).

2. Guidance on the Security Assessment of Generic New Nuclear Reactor Designs, CNS-TAST-GD11.1, Issue 1.2, May 2021 (Reference [12]).

3. New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-007 Revision 0, May 2019 (Reference [13]).

2.4.16 The expectation of the ONR is that a GDA nuclear security submission should be primarily in the form of a GSR. This guidance makes specific reference to the requirement that the GDA GSR:

> "….must be able to meet regulatory expectations, in respect of Security Assessment Principles (SyAPs) Fundamental Security Principles (FSyPs), in order that a future site-specific security plan can be developed".

2.4.17 ONR Guidance (Reference [12]) also states that:

> "The objective for the security assessment of the generic design is for ONR to judge whether the proposed arrangements will be adequate to address relevant threats and are capable of being, and likely to be, successfully integrated into the overall site arrangements."

2.4.18 We will develop a GSR which will seek to demonstrate to the ONR that our proposed security arrangements successfully address the relevant threats. This GSR will be presented in the form of a 'claims-arguments-evidence' approach.

2.4.19 The proposed development of a GSR to deliver against these requirements, as the RR SMR progress through GDA is discussed in the Section 3 of this PSyR.

ONR CNSS Technical Assessment Guides (TAGs)

2.4.20 ONR CNSS has developed a series of nuclear specific TAGs. These TAGs cover a range of individual security topics which provide more detail of (and cross-reference with) the expectations set out in the FSyPs. As appropriate, these TAGs refer back to internationally accepted good practice as outlined in corresponding IAEA guidance.

2.4.21 These TAGs are intended to aid ONR CNSS inspectors in the undertaking of their regulatory duties with regard to operational nuclear installations and are not specific to GDA. Nevertheless, they provide information which is useful to the development of the RR SMR and will be consulted as appropriate.

2.4.22 A full list of relevant TAGs is not included here. Rather, relevant TAGs will be referenced as appropriate elsewhere in this PSyR.

3 Generic Security Report

3.1 Introduction

3.1.1 As outlined in the ONR guidance to RPs (Reference [1]), the main GDA nuclear security submission will be in the form of a GSR, together with supporting documents and information.

3.1.2 This section of the PSyR sets out our initial proposals for the development of the GSR.

3.1.3 The final version of the GSR should be sufficient to form the basis of the NSSP to be developed by a future NSL holder.

3.1.4 Initially, as outlined in the subsequent sections of this PSyR, the focus of the GSR will be on addressing the expectations of the ONR regarding the following relevant SyAPs (Reference [2]):

1. Fundamental Security Principles (and associated delivery principles) –
    a. FSyP 5, Reliability, Resilience and Sustainability
    b. FSyP 6, Physical Protection System
    c. FSyP 7, Cyber Security and Information Assurance.
2. Key Security Plan Principles –
    a. KSyPP 1, Secure by Design
    b. KSyPP 2, The Threat
    c. KSyPP 3, The Graded Approach
    d. KSyPP 4, Defence In Depth
    e. KSyPP 5, Security Functional Categorisation and Classification
    f. KSyPP 7, Codes and Standards.

3.1.5 Later versions of the GSR will also need to address other relevant SyAPs (FSyP 5-Reliability etc., FSyP 9 – Policing & Guarding, and FSyP 10 – Emergency Preparedness etc.), which would be addressed in more detail as part of a subsequent (to GDA) nuclear site licence application and the development of a NSSP. At GDA, this would be addressed through the inclusion of a 'Concept of Operations' within the GSR, demonstrating that the RR SMR has considered the (non-site specific) delivery, and operational phase requirements.

3.1.6 The intention is that the GSR document will be drafted such that none of the information contained within should be classified as SNI or otherwise as Official-Sensitive or Secret. SNI etc. will be presented in dedicated topic reports. This

approach will also aid in the controlled release of security information as part of the public consultation exercise.

3.2 Development of the GSR with Design Maturity

3.2.1 The relationship between GSR versions and the Reference Design Points (see Paragraph 1.3.3 is anticipated to be:

1. GSR Version 0– Preliminary Concept Definition Phase 2 (PCD2)
2. GSR Version 1 - Full Concept Definition (FCD)
3. GSR Version 2 – Full Concept Definition (FCD) and/or Developed Design
4. GSR Version 3 (Final) - Developed Design (DD).

3.2.2 Each successive version of the GSR will be updated to reflect design maturity and any impacts that such has on the development of the security solution for the RR-SMR.

3.2.3 All four versions of the GSR will be supported by topic reports and other references as necessary.

3.2.4 One of the topic reports, which will be regularly updated, will be a 'map' of the nuclear security submission against the relevant SyAPs.

3.2.5 At this stage, we anticipate that the four iterations of the GSR, will cover the following:

1. **GSR Version 0** – this version will expand the nuclear security claims presented in the PSyR and start to layout the justifying arguments; there is likely to be only limited substantiating evidence presented.
2. **GSR Version 1** – this version will present an expanded set of claims (to include, at least Level 2), the evolving arguments and start to present or point to the substantiating evidence.
3. **GSR Version 2** – this version will present a near complete set of claims and arguments and either present or point to the substantiating evidence.
4. **GSR Version 3 (Final)** – this version will present the finalised nuclear security submission, taking into account the comments received from the ONR throughout GDA.

3.3 Outline of Content & Structure of the GSR

3.3.1 The GSR will present the generic security arrangements for the RR SMR and substantiate such against the high-level security claims (which are presented in Section 6 of this PSyR) and the subsequently developed lower level claims.

3.3.2 The GSR will be developed and presented with a 'claims-argument-evidence' structure (CAE), which will be common across E3S as a whole. This is discussed further in Section 4.

3.3.3 This CAE approach will substantiate the security arrangements for the RR SMR against the security objectives and principles that are outlined in Section 5 of this PSyR.

3.3.4 The Fundamental and Level 1 nuclear security claims that will form the basis of the GSR are introduced in Section 6 of this PSyR, together with an indication of how the overall structure of the 'claims-argument-evidence' will be developed as the design of the nuclear security solution matures. These Level 1 claims are based around the SyAPs which will be the main focus of the GSR.

3.4 Governance of GSR

3.4.1 Rolls-Royce SMR is developing a governance and assurance framework and Integrated Management System (IMS); such will meet the needs of the business, using shared best practices with strong links back to the Rolls-Royce code of conduct, governance framework and policies.

3.4.2 The Governance and Assurance Framework and IMS enables RR SMR to manage risk, drive critical business decisions, and maintain and assure standards across the business.

3.4.3 As part of this framework, the Chief Executive Officer (and wider Executive Leadership Team) will be able to seek advice from the Rolls-Royce SMR Design, Safety and Environment Advisory Committee (DSEAC).

3.4.4 This advice will be provided by senior independent technical experts, in relation to subject matters including: design philosophy, nuclear safety, radiological environmental protection, and security in relation to the proposed design and layout of, and the associated E3S case developed to support the development of the design.

3.4.5 The DSEAC is a formal advisory committee within the Rolls-Royce SMR governance structure and operates in accordance with an endorsed set of Terms of Reference (TOR) which define how documents and information must be supplied and presented to the Committee. The Committee provides independent advice on the top-level documents of the E3S case.

Governance – E3S (including Nuclear Security)

3.4.6 As with all other aspects of RR SMR delivery, E3S activities are subject to appropriate programme and project management which ensure the consistent application of technical and managerial standards to E3S activities. How this is applied within E3S is set out in the E3S Management Manual [14].

3.4.7 Governance over E3S activities in RR SMR is the responsibility of the Executive Director for Regulatory Affairs, with delegation to Heads of Function as necessary and appropriate.).

3.4.8 The Executive Director is supported by an internal Nuclear Assurance Function which is independent of the E3S case delivery. Nuclear Assurance will deliver this function, in part, through the Safety Advisory Committee.

Governance of E3S Case Documentation (Including Nuclear Safety)

3.4.9 All E3S case documentation will be subject to the following governance which is mandatory:

1. **Technical Check** – undertaken by competent person working for Rolls-Royce SMR, who is independent of the Author to ensure input data is accurate, appropriate methodologies have been applied and any conclusions and/or recommendations made are supported by the information presented. A technical check shall also include review by any relevant stakeholders.

2. **Approval** – Approval is given by the E3S Manager (or delegate, e.g. Head of Security) to confirm that document has been prepared in accordance with all required procedures and standards, is fit for purpose and has had all required technical review governance carried out.

3.4.10 Members of the E3S team are the Intelligent Customer (IC) for the acceptance of external work packages (i.e. from the supply chain organisations). This will ensure the document is valid, uses suitable methodologies (in line with E3S principles) and fulfils its intended purpose. The expectation is that such document will have also been subject to appropriate governance within the supply chain organisations.

3.4.11 All E3S documents are categorised in line with the E3S Categorisation Guidance document, see Reference [15] (Rolls-Royce SMR E3S Guidance on Document Categorisation). The document category determines the governance route and assurance levels for documents that support the E3S cases. Depending on the categorisation of the document additional assurance may be undertaken.

3.4.12 Further detail on governance can be found in the documents referenced in this Sub-section and in other references therein.

4 Development of the E3S Case

4.1 Introduction

4.1.1 As noted in Paragraph 1.3.10, Rolls-Royce SMR are promoting an integrated E3S approach to the development of the Safety, Environmental Protection, Security and Safeguards cases.

4.1.2 To support this and to provide for a consistent approach to the presentation of the individual case through the CAE approach, an E3S Case Strategy (Reference [16]) has been developed.

4.1.3 This high-level CAE approach will help to ensure a logical structure for the overall E3S Case, that:

1. Provides traceability from the overall E3S objective down through to the detailed Evidence in a structured manner (the golden thread).

2. Provides a clear purpose for each Evidence item by relating it to the Sub-Claim(s) it is intended to satisfy.

3. Provides confidence in the completeness of the case, with gaps easily identified.

4.1.4 The E3S Case Development Strategy sets out how E3S case(s) will interface and align with GDA engineering design reference points (see Paragraph 1.3.3). This alignment ensures that the design definition and rationale outputs, which forms part of the Evidence to be captured within the E3S Case, will support the justification that risks are reduced to ALARP, in line with Best Available Techniques (BAT) and are Secure by Design (SyBD).

4.2 E3S Case Strategy

4.2.1 E3S are key stakeholders in the systems engineering design processes to ensure that the iterative development of the E3S Case evidence supports a balanced demonstration of As Low As Reasonably Practicable (ALARP), BAT and SyBD.

4.2.2 The E3S Case Development Strategy (Reference [16]) describes the development of the overall E3S Case to support the design phase of the programme. This includes development of the structured E3S case to be submitted to the GDA.

4.2.3 This E3S strategy provides the high-level framework for development of the E3S Case. The E3S Case refers to the totality of documentation/data that justifies RR SMR achieves its fundamental objective to 'protect people and the environment from harm'.

4.2.4 A CAE approach has commonly been adopted in structuring Safety Cases in the UK for both nuclear and non-nuclear safety critical industries. Both the ONR SAPs (Reference [11]) and SyAPs (Reference [2]) indicate an expectation for Safety and Security Cases respectively to set out the trail from claims, through arguments, to evidence (i.e. the 'Golden Thread'). However, such a CAE approach is not mandatory, and the presentation of CAE is not prescribed.

4.2.5 Effective construction of a CAE structured case is typically achieved by devising appropriate claims in a hierarchical manner, initially top-down from the overall objectives.

4.2.6 The top-level claims are broken down, typically, via arguments into a sets of sub claims, to a level that links directly to an evidence item that satisfies it. This is represented at a basic level in Figure 2. Sub-claims can also be derived through a combined top-down and bottom-up approach, which aids in the alignment with both objectives and evidence sources.

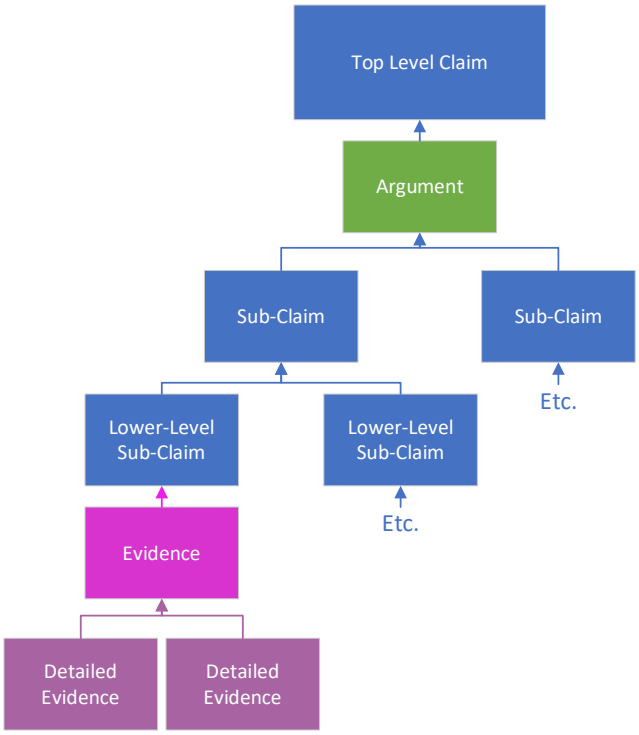


Figure 2 – Basic CAE Structure for RR SMR

4.3 E3S Case Hierarchy

4.3.1 The E3S Case for RR SMR will be developed in a hierarchical manner, comprising the following 'tiers' of information:

1. **Tier 1**: a top tier submission for each of the E3S disciplines, providing an overarching summary and entry point to the evidence located in the lower tiers. The level of detail will be summarised such that it is meaningful when read in isolation, but will signpost to evidence on Tier 2 for an increased level of detail.

2. **Tier 2**: the first level of underpinning arguments and evidence, comprising a set of more detailed summary documents that can be easily referenced from the Tier 1 report, and also signpost out to the detailed evidence on Tier 3.

3. **Tier 3**: the detailed evidence for different aspects of the E3S Case, that supports and is referenced from the Tier 2 summary documents.

4.4 Assurance & Safety Case Environment (ASCE) Software

4.4.1 Electronic tools and software are available that can support the structuring and communication of a safety and assurance cases using a more 'digital' approach than a traditional collection of reports and references.

4.4.2 Rolls-Royce SMR is embracing the use of such tools to facilitate development of the E3S Case. Rolls-Royce SMR has selected the use of ASCE software (developed by Adelaard) for the E3S Case. An example is shown on Figure 3.

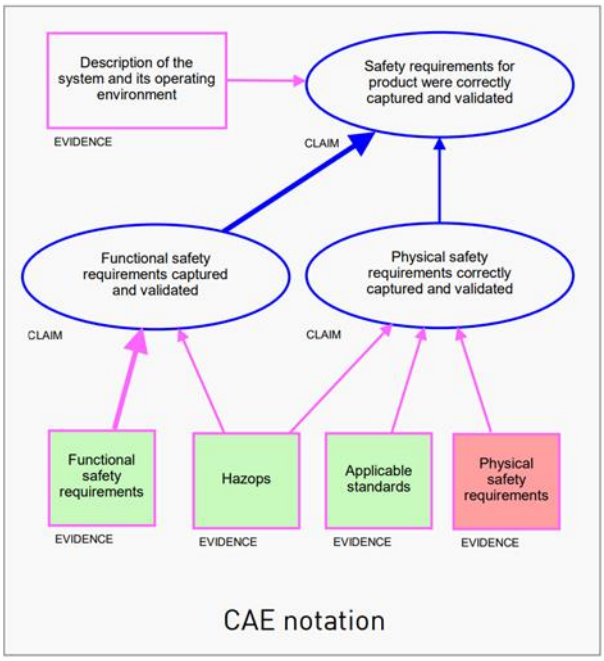


Figure 3 – Example ASCE Presentation of CAE

4.5 Nuclear Security Case (GSR)

4.5.1 The security solution for the RR SMR will be developed to achieve the security objectives outlined in Sub-section 5.2 through the application of the security principles presented in Sub-section 5.3.

4.5.2 The Tier 1 report will be the Generic Security Case (GSR). The GSR will adopt a CAE structure (as for E3S as a whole) and will be based around. The high-level security claims that will form the basis of the GSR structure are set out in Section 6.

5 Security Objectives & Design Principles

5.1 Introduction

5.1.1 Objectives and design principles form of basis of effective systems engineering and design. These objectives and principles are decomposed into functional design requirements and eventually detailed specifications. These principles and their decomposition provide a measurable baseline against which design options can be evaluated.

5.1.2 A similar systems engineering approach is adopted for the design of the security arrangements for the RR SMR. However, the approach to nuclear security is risk-informed rather risk-based; that is the approach is cognisant of the risks, but will not disregard security risks which have a very low probability of occurrence.

5.1.3 This section sets out the objectives and design principles that have been adopted to inform nuclear security for the RR SMR. There is also a brief discussion of the typical security functions that will deliver these objectives.

5.1.4 As highlighted throughout this PSyR document, nuclear security is fully integrated into engineering design and has much in common with the approach to nuclear safety. An introduction to how this integration works is also set out in this section.

Fundamental E3S Objective

5.1.5 Regulation of the UK civil nuclear industry covers the topic areas of environmental protection, nuclear safety, nuclear security and safeguards. Rolls-Royce SMR has set out to ensure that there is an integrated approach to the delivery of these three topic areas (as far as is practicable) in the RR SMR design.

5.1.6 The overarching common aim for the E3S topic areas is to protect people and the environment from potential sources of harm.

5.1.7 From the point of view of E3S, the fundamental objective of the design of the RR design is…

> '…to protect people and the environment from harm (Reference [17]).'

5.1.8 Whilst there is significant commonality of approach and design between the E3S disciplines, there is also the recognition of competing priorities.

Potential Sources of Harm

5.1.9 When considering the potential sources of harm associated with a nuclear power station, these fall into two groups (as shown on Figure 4):

1. Nuclear – that is harm that can result from exposure to ionising radiation.

2. Conventional – all other source of harm, e.g. physical, chemotoxic etc.

5.1.10 The RR-SMR is designed and operated to control and reduce risks from both nuclear and conventional sources of potential harm. Clear parallels exist between the E3S disciplines, with common fundamental objectives.

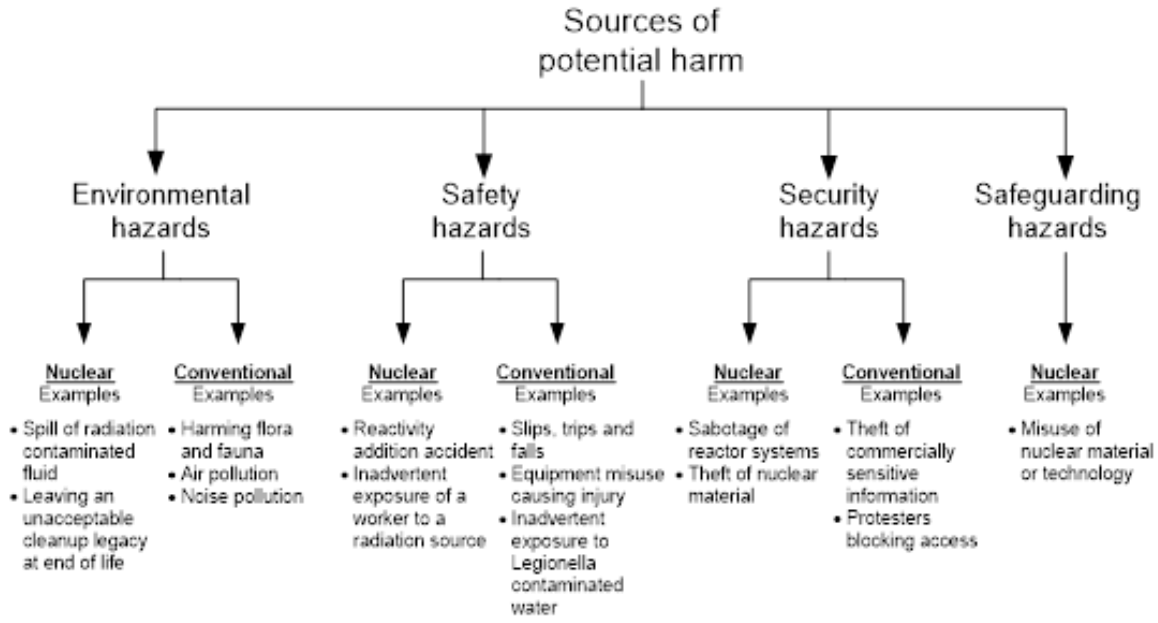


Figure 4 - Nuclear Power Plant Sources of Potential Harm

Risk-Informed

5.1.11 In alignment with the approach in the UK, the RR SMR will adopt a risk-informed approach to nuclear security rather than a strictly risk-based one. Such an approach is typically required by regulatory regimes around the world and corresponds with the Outcome-based approach to nuclear security in the UK.

5.1.12 The security arrangements will aim to address all credible design basis risks rather than just those which exceed a risk baseline based on frequency and consequences. Nevertheless, a proportionate approach will be taken in protecting against these design basis risks.

5.2 Security Objectives – Nuclear and Conventional

5.2.1 One of the commercial objectives of Rolls-Royce SMR is that it will be available not just for construction within the UK but also for export and construction internationally. To support this commercial objective, the design of the security arrangements must be adaptable to differing regulatory regimes both permissive and prescriptive.

5.2.2 The nuclear security objectives for the RR SMR set the high-level security requirements that inform engineering design decisions (see Sub-section 5.5).

5.2.3 The Rolls-Royce SMR nuclear security objectives reflect the moral obligation to protect people and the environment from harm (both conventional and nuclear) and

are not just the (typically) more limited set of regulatory obligations (which are concerned primarily with nuclear security[1]).

5.2.4 Furthermore, regulatory obligations are not necessarily concerned with the secure protection of all on-site assets; there are commercial imperatives on the security of the RR SMR which might not be of concern to regulators, but which are drivers of engineering design (for example, availability of electricity generation, protection of intellectual property rights). Regulatory and commercial imperatives are not necessarily exclusive.

5.2.5 Taking into account the above discussion, the high-level security objectives for the RR SMR that primarily address **nuclear harm and/or regulatory obligations** are:

1. **To assure nuclear security** – The security arrangements for the RR SMR will meet our moral obligations to protect people and the environment from harm and be compliant with the relevant regulatory regime for nuclear security.

2. **To prevent malicious acts which could result in Unacceptable Radiological Consequences** – The primary purpose of nuclear security is the prevention of harm arising from either the sabotage or of theft of NM/ORM.

3. **To prevent compromise of Sensitive Nuclear Information** – The protection of information relating to the security, design and operation of the RR SMR power station could aid the execution of malicious acts such as theft and sabotage.

5.2.6 Considering the above discussion, the high-level security objectives for the RR SMR that primarily address **conventional harm and or commercial imperatives** are:

1. **Global deployment** – The security arrangements for the RR SMR will be readily adaptable to allow for global deployment and compliance with both permissive and prescriptive regulatory regimes. This will consider differing regulatory requirements and the imperative to protect commercial assets and operations.

2. **Protect the availability of generation** – The economic sustainability of the power station is dependent on its ability to generate energy. Extended or frequent disruption of generation could threaten the economic sustainability of the power station.

3. **Protect personnel and plant from internal and external threats** – The power station operator will have a duty of care to protect its employees and visitors, and a vested interest in protecting its fixed assets, from external threats that may wish to cause harm, damage equipment or theft of valuable items.

5.3 Security Principles

5.3.1 The E3S Function has defined a series of E3S Fundamental Principles Reference [17]. These provides a design framework whereby the RR SMR is evaluated and developed to ensure that it will operate safely and securely.

[1] As discussed in Section 2

5.3.2 The Fundamental Security Principle is as follows:

> Prevention and detection of and response to, theft, sabotage, unauthorised access, illegal transfer or other malicious acts involving nuclear matter or compromise of sensitive nuclear information shall be enforced.

5.3.3 The design and operation of the RR SMR should ensure 'security by design' whereby vulnerabilities are eliminated or reduced by design rather than secured or mitigated with measures. Inherent security should be achieved through the application of the hierarchy of controls (Figure 3). Where inherent security is not reasonably practicable, security measures should be provided.

5.3.4 The security objectives for the RR SMR will be delivered through the application of the SMR Security Principles (SSyPs) which are set out below. The derivation of these security principles is in line with the wider development of E3S principles (Reference [17]) and consistent with the expectations of the ONR SyAPs (Reference [2]).

5.3.5 These SSyPs apply throughout the engineering design process and put requirements on all engineering disciplines.

SSyP 1 – Minimise Inherent Risk

5.3.6 This SSyP seeks to minimise the security risk that is inherent in the design (before applying dedicated security controls) for example by:

1. Applying a security by design approach to engineering design.

2. Limiting the quantity of nuclear material used and stored on site to the minimum required to support operations.

5.3.7 An effective route to achieving an inherently secure facility, i.e. one with the minimum inherent security risk, is to apply a hierarchy of security controls. This hierarchy begins with elimination as the most preferable and effective; with operational/human factors as the least preferable and highest cost means of controlling a security risk. This is illustrated in Figure 5.

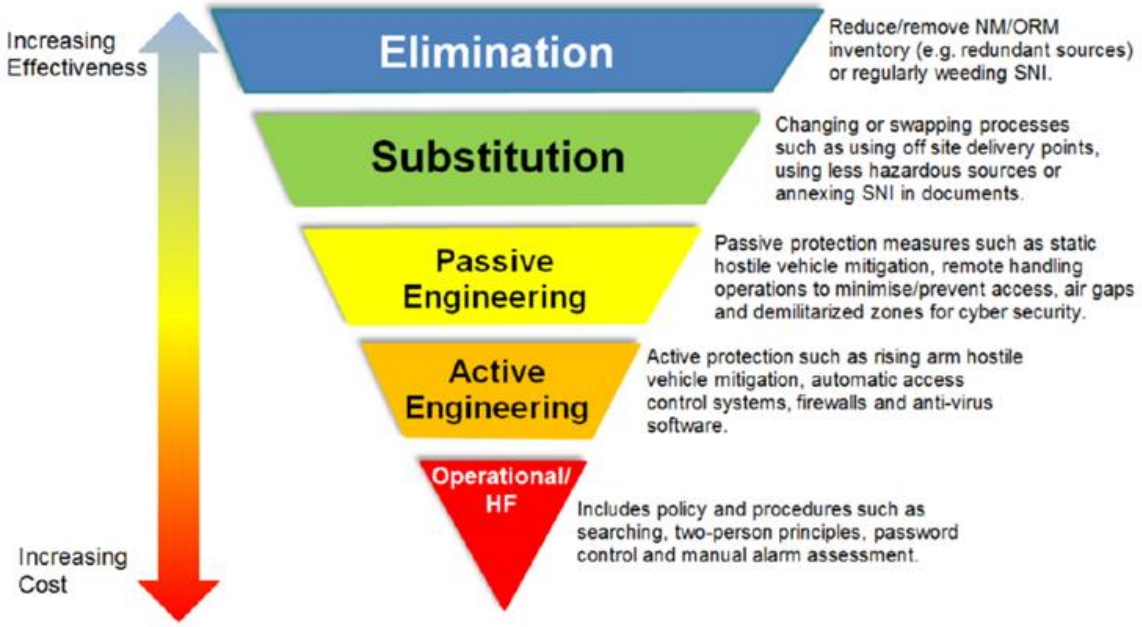


Figure 5 - ONR SyAPs Security Hierarchy of Controls (ONR 2017)

5.3.8 The design process will prioritise the elimination or reduction of security risk at source before considering the application of dedicated controls to manage a risk. This will result in a design that is inherently secure, thus requiring the least amount of additional, dedicated security measures that would otherwise add to construction and operational costs of the power station.

SSyP 2 – Demonstrably Secure Designs

5.3.9 While the aim of design activities is to achieve a security solution that meets requirements, the effectiveness of the solution must be demonstrated and/or substantiated.

5.3.10 When selecting concept security solutions, designers will consider whether claims relating to the performance of the chosen concept can be substantiated. Where performance of a given concept solution cannot be demonstrated, it will not be possible to use the related claims in the GDA nuclear security submission for the RR SMR.

SSyP 3 – Through-Life Assurance

5.3.11 This SSyP seeks to ensure that RR SMR has the necessary features designed-in to demonstrate, with a high-degree of confidence, that the power station meets its security requirements now and will continue to meet those requirements throughout its life.

5.3.12 The RR SMR programme has a long lifetime, spanning from its initial concept design to the eventual decommissioning of the first build, approximately 75 years later. This long lifecycle will be punctuated by periods of alternative phases of operation and non-operation, e.g. for construction, maintenance, refuelling or decommissioning (see Figure 6).

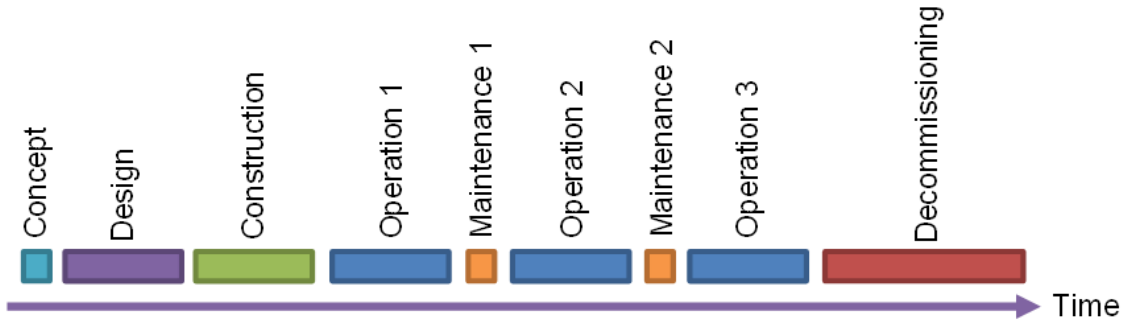


Figure 6 - Example Facility Lifecycle

5.3.13 Designers will consider the security needs of the RR SMR throughout its lifecycle, from concept to decommissioning. The security needs of the facility are likely to be different at each of these stages, and designers may need to design in features to accommodate these needs. Security arrangements must also ensure that the security systems are sustainable and can be modified or expanded to meet future threats.

5.3.14 Throughout the life of the power station, evidence will be sought that the security of the facility has been designed, implemented and operated correctly, and achieves appropriate levels of resilience and reliability. This evidence is then used to provide through-life security assurance.

SSyP 4 – Economically Sustainable Security

5.3.15 This SSyP seeks to ensure that the security arrangements for the RR SMR are economically sustainable throughout the life of the power station by facilitating the operation and maintenance of the power station while maintaining the required levels of protection.

5.3.16 In addition to protecting the public from harm, the security arrangements for the RR SMR must also protect the financial interests of the operator; that is ensuring that the power station remains an economically sustainable venture. Security-related threats to economic sustainability come from disruption to operations, threats to staff safety, or damage to or loss of assets. Protecting against these threats may require investing in security beyond the regulatory requirements. This economic protection will seek to:

1. Protect the availability of the power station to produce energy for sale.
2. Protect non-nuclear power station assets from theft or sabotage.
3. Prevent or minimise disruption due to external non-environmental effects such as anti-nuclear protests.
4. Facilitate the operation and maintenance of the power station while maintaining the required levels of protection.
5. Minimise the cost of security throughout the power station's life while maintaining the required levels of protection.

5.3.17 Assessment of the cost of security, and efforts to minimise it, will span the entire life of the power station. For example, designing-in features to facilitate maintenance of security systems creates up-front costs but can reduce the total cost of maintenance through life.

SSyP 5 – Globally Deployable

5.3.18 This SSyP seeks to ensure that the security arrangements for RR SMR are deployable internationally as well as in the UK.

5.3.19 To achieve this, the security arrangements will be designed around a core of requirements that are compliant with most international regulatory regimes, i.e. the IAEA Nuclear Security series of publications, with extensions and adaptions to meet local regulations.

5.4 Security Functions

5.4.1 The security objectives and principles are embedded into engineering design through the designation of appropriate security functional requirements.

5.4.2 The security arrangements that deliver these security functions will include: physical security systems, cyber security, procedural/behavioural controls, and human actions – or a combination of any or all of such.

5.4.3 Typically, the security functions used to inform engineering design may include:

1. **Deter** – Security arrangements that give the impression to a would-be threat actor that an attempt to subvert the security of the facility is unlikely to succeed, or that the cost of undertaking a malicious act would outweigh any benefit (i.e. they are likely to be caught or killed during the act).

2. **Detect** – Security arrangements that provide a timely indication to responders that a malicious act is underway or is likely to occur.

3. **Delay** - Security arrangements that increase the time that a threat actor must invest in the commission of a malicious act, increasing the probability of detection and the opportunity for response.

4. **Control Of Access** – Security arrangements which control authorised access and seek to prevent and/or detect unauthorised access.

5. **Insider Threat** – Security arrangements which seek to identify and prevent malicious actions by persons with authorised access.

6. **Assess** – Security arrangements that collect and collate information on which to base a response or initiate mitigation.

7. **Respond** – Security arrangements which aim to prevent the progression of an attack sequence, e.g. through interdiction by an armed guard force.

8. **Mitigate** – Security arrangements that aim to recover control over a security incident, for example the execution of emergency plans.

5.4.4 Examples of the security arrangements that can deliver some of these security functions are illustrated on Figure 7. In practice, a combination of security function types is needed to achieve defence in depth.

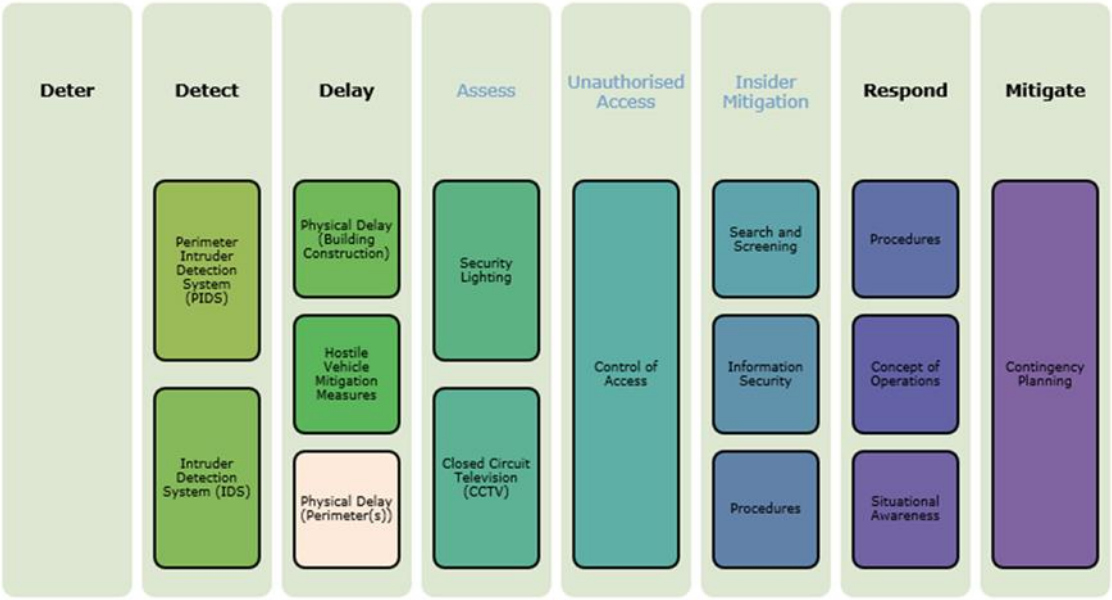


Figure 7 - Layered Arrangement of Security Functions

5.4.5 Security functions will be delivered as far as possible through the use of passive and/or integrated (intrinsic) security arrangements rather than reliance on active and or dedicated (extrinsic) security arrangements.

5.4.6 SSCs are not typically provided simply to provide a deter function. Rather, the individual, and combination of visible SSCs which fulfil the security requirements provide a comprehensive, integrated security solution and in so doing deliver an overall deterrence.

5.5 Integration of Nuclear Security into the RR SMR Design

Engineering Design

5.5.1 Traditionally, reduction in nuclear security risk has been achieved through applying dedicated security controls (extrinsic security) to a fully developed nuclear power station; however, UK nuclear industry experience has shown that the application of such 'traditional' security measures might not be the most optimal solution in treating the identified risk.

5.5.2 Rolls-Royce SMR is seeking to adopt a Secure by Design[2] approach whereby:

1. Preliminary (high-level) security requirements are identified at the concept stage of design and integrated into the overall engineering requirements process (see paragraphs 5.5.8 to 5.5.10). more detail.

[2] See Section 7

2. The appropriate security arrangements are developed alongside the maturing engineering design and supported by the integration of more detailed requirements.

5.5.3 The approach seeks to reduce security vulnerabilities within the engineering design (i.e. 'intrinsic security') and identify the (more traditional) security measures necessary to address the residual vulnerabilities (i.e. 'extrinsic security').

5.5.4 The design of extrinsic security arrangements will also follow a requirements led secure by design process whereby the chosen options are substantiated rather than '*just what has been used previously*'.

5.5.5 The successful application of a Secure by Design approach will:

1. Encourage efforts to reduce security risk at source, before considering the effect of a security protection system.

2. Adopt a system-level, or systems engineering, approach to the design of nuclear security arrangements.

3. Engineer features into the design of the SSCs that have security functionality.

4. Encompass the entire lifecycle of the facility.

5.5.6 Designing security into SSCs requires specialist knowledge and competence with security analysis and risk management tools. This approach requires security Subject Matter Experts (SMEs) to work alongside designers and engineers in order to ensure the integration of security functionality and requirements into the design of the RR SMR. As the design moves out of the concept phase, Rolls-Royce SMR will continue to develop tools and processes which enable this integration and measure it effectiveness. Example tools will include a Security Engineering Schedule, which will be developed alongside a process for security functional categorisation and classification (see Paragraph 8.4.9 to 8.4.20). This schedule will form the interface between the security analyses and engineering design processes.

5.5.7 Requirements are the currency of engineering design. To successfully integrate nuclear security with the main engineering design process of the RR SMR, nuclear security has (and will continue) to place security requirements into the engineering design process (see Reference [18]).

5.5.8 At a high (concept) level, these security requirements will relate to the Fundamental Security Principle (paragraph 5.2.3) and the interpretation of the UK Design Basis Threat (DBT). As the design process moves from concept toward detail, the output from the various security analyses will lead to the development of increasingly detailed design; for which more detailed requirements might be in the in the form of the security functions discussed above.

5.5.9 Rolls-Royce SMR has adopted the use of IBM Dynamic Object-Orientated Requirements System (DOORS) for requirements management. Each SSC has will have its own dedicated DOORS modules within the DOORS database, covering requirements specification, design definitions, and verification strategies. The database enables links between these modules, providing traceability of design information.

5.5.10 The functional and non-functional requirements derived through the E3S Case (including security) will feed into this requirements management process in DOORS, thus providing a 'digital' golden thread between the requirements derivation in the E3S Case analysis and the associated engineering substantiation.

Nuclear Safety

5.5.11 The aims of nuclear safety and nuclear security are complementary; in that both aim to reduce the risk of harm to people and the environment. Hence some protective measures that adequately address the requirements of nuclear safety should also satisfy the requirements for nuclear security.

5.5.12 Nuclear safety is concerned with accident fault sequences that could be randomly triggered by initiating events, which include equipment failure, human actions and naturally occurring external hazards. Nuclear security, however, is concerned with initiating events of malicious origin (IEMOs) which could intentionally trigger accident fault sequences and the loss of safety functions (criticality, cooling, confinement).

5.5.13 Whilst a common approach is preferable, on some occasions a common solution will not be possible or practicable, and it is appropriate to arrive at solutions that address the requirements of nuclear safety and security separately. In such circumstances, priority will generally be given to nuclear safety concerns, with the security risk addressed by extrinsic arrangements.

5.5.14 Given this complementary relationship between safety and security, the Secure by Design approach that has been adopted for the RR SMR seeks to bring the GDA nuclear safety and nuclear security submissions into close alignment; to the extent that a large part of the evidence that substantiates both submissions will be shared. This is the philosophy behind the E3S approach (see Section 4).

5.5.15 The integration between the nuclear safety and nuclear security is perhaps best illustrated in the process for identifying vital areas (see Sub-section 8.2). This in effect seeks to match potential malicious actions to the initiating event (IE) (for accidents sequences) in the safety case in order to identify that which could result in URCs.

5.5.16 Both nuclear safety and security perform area categorisation activities to aid definition of the requirements for protection. An integrated approach offers the opportunity for increased alignment and consistency (for example, between identified Vital Areas and radiological protection zones).

5.5.17 In addition to recognising the similarities between nuclear safety and security, it will also be important to recognise where there are significant differences. The most significant difference is that whereas nuclear safety utilises both deterministic and probabilistic analyses nuclear security is much more deterministic in nature. This is part of the risk informed approach to nuclear security.

5.5.18 For example, nuclear safety analyses take into the account the probability/frequency of an IE occurring; and, where an IE has a sufficiently low frequency of occurrence, it may be determined that preventative or protective safety measures are not required. That is, probabilistic assessment informs whether or not safety measures are necessary.

5.5.19 With regard to security, the security arrangements must be able to protect against the UK DBT. Hence, for the purposes of security analysis, a conservative approach is adopted; whereby it is generally assumed that if an IEMO could result in either a URC or theft of nuclear material, preventative or protective measures must be provided. No account is taken of the probability of such an IEMO occurring.

6 Nuclear Security Claims

6.1 Introduction

6.1.1 The GSR for the will comprise a logical and hierarchical set of documents that:

1. Analyses the risks that could arise from malicious actions which could conceivably result in URCs.

2. Addresses these risks with regard to the modes of operation and potential vulnerabilities of a nuclear site.

3. Identifies the security arrangements that need to be implemented to prevent or mitigate these risks.

6.1.2 The GSR will present a balanced view and understanding of the security risks and provide a proportionate view of the level of security to address such. The justification for these security arrangements will include appropriate conservatism but without undue pessimism.

6.1.3 Rolls-Royce SMR will seek to take account of experience and good practice from within the Security Team and the wider civil nuclear industry. The production of a security plan does not in itself ensure the security of a nuclear site; rather, it sets expectations and guidance for the processes that should operate in the future if security is to be delivered successfully.

6.1.4 In line with the transition (in the UK) to an outcome-based approach to nuclear security, emerging good practice is to present a nuclear security submission in a CAE structure. This should clearly articulate and demonstrate the linkage from security claims through arguments to the evidence underpinning the claims. This structure mirrors the well-established way nuclear safety cases are presented; and should aid in the close integration between nuclear security and safety.

6.1.5 The GSR will adopt a CAE structure (as discussed in Section 4).

6.1.6 This section of the PSyR presents the higher-level claims that will form the basis for the subsequent GSR.

6.1.7 Subsequent sections (Sections 7, 8 and 9) of this PSyR discuss the topics covered in these claims and set out the basics that will form the arguments that will justify these claims. These arguments will be developed as the nuclear security arrangements are developed.

6.2 Nuclear Security Claims

6.2.1 Set out below are the Fundamental Nuclear Security Claim and the supporting Level 1 security claims that will form the basis of the GSR for the RR SMR.

6.2.2 As the GSR progresses, the Level 1 claims will be subject to review to reflect the increasing maturing of the engineering design.

6.2.3 The Level 1 claims will be unpinned by relevant and appropriate lower-level claims (Level 2 and Level 3). This PSyR does not seek to discuss these lower-level claims in any detail. The development of these lower-level claims may also need to be reflected in revised wording of the higher-level claims.

Fundamental Nuclear Security Claim

6.2.4 This fundamental claim mirrors and supports the fundamental E3S objective for the RR SMR (see Sub-section 5.1).

> **[NSy 0] 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.

6.2.5 This fundamental claim recognises the objective for international deployment of the RR SMR.

Level 1 Security Claims

6.2.6 The Level 1 nuclear security claims are derived from the RR SMR security objectives (see Section 5). As discussed in Sub section 4.2, these objectives can be grouped into those that are primarily to address regulatory obligations and those which address commercial imperatives. Only those primarily concerned with regulatory obligations are taken forward. Likewise, the claims are concerned with nuclear and not conventional harms.

6.2.7 At this level, the claims have also started to become more UK specific rather than internationally facing (as for the fundamental security claim).

6.2.8 This approach reflects the purpose for which this PSyR has been produced and the regulatory regime under which the GSR will be assessed initially.

6.2.9 Further, these high-level claims aim to address the major security topics expected to be addressed by the GSR, i.e. sabotage, theft and protection of SNI. These claims will be suitable to be carried forward into any (UK) NSL application. 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'.

6.2.10 The Level 1 security claims are:

> **[NSy 1.0] Secure by Design:** The protection from harm provided by the nuclear security arrangements will be risk informed, cognisant of and proportionate to the UK DBT and integrated into engineering design; through an approach that seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design. Alignment with the expectations of the relevant ONR SyAPs will ensure that the nuclear security solution is adoptable by prospective future nuclear site licence holders.

[NSy 2.0] Protection from Sabotage: As far as is reasonably practicable, the PPS will prevent malicious acts of sabotage which could result in Unacceptable Radiological Consequences. The PPS will deliver the security functions of 'Deter', 'Detect', 'Delay', 'Assess', 'Control of Access', and 'Insider Threat' – in order to address the relevant design basis threat.

[NSy 3.0] Protection from Theft: As far as is reasonably practicable, the PPS will prevent the theft of nuclear/radiological material or compromise of Sensitive Nuclear Information. The PPS will deliver the security functions of: 'Detect', 'Delay', 'Assess', 'Control of Access, and 'Insider Threat' - in order to address the relevant design basis threat.

[NSy 4.0] Cyber Security & Information Assurance (CS&IA): The focused application of CS&IA as part of a larger Cyber Protection System (CPS) will prevent malicious acts to all digital assets (including Operational Technology [OT] and Information Technology [IT]) or interruptions to services that could foreseeably result in: Unacceptable Radiological Consequence, the theft of nuclear/ radiological material or the compromise of sensitive nuclear information. The CS&IA will deliver the functions of: 'Detect', 'Delay', 'Resist' and 'Recover' - in order to address the relevant design basis threat.

6.2.11 The outline approach to how these high-level claims (and subsequent supporting lower-level claims) will be substantiated as the GSR develops is discussed in this PSyR as follows:

1. [NSy 1.0] Secure by Design – see Section 7
2. [NSy 2.0] Protection from Sabotage - see Section 8
3. [NSy 3.0] Protection from Theft - see Section 8
4. [NSy 4.0-] Cyber Security & Information Assurance (CS&IA) -*see Section 9*.

6.3 Nuclear Security Case – Architecture

6.3.1 It is not the purpose of this PSyR to present a full set of CAE - these will develop as the engineering design (incorporating the security solution) advances.

Claims

6.3.2 The nuclear security claims that form the skeleton of the GSR submission will continue to be developed as it matures.

6.3.3 The architecture of the Level 1 claims and supporting lower-level claims will be structured and drafted on the basis of the following (which will be followed as far as is possible):

1. Level 1 claims should be capable of supporting a through lifecycle security case – lower-level claims may only need to support specific lifecycle stages or operating conditions.

2. Level 2 & 3 claims should support relevant higher-level claims, but (as far as possible) should be independent of other claims at the same level (i.e. a vertical rather than horizontal architecture).

3. Claims should align with other equivalent E3S claims (as far as is possible and recognising differences between the disciplines).

4. Claims should be self-contained and focused (i.e. deep not wide).

5. Claims should be bounded as necessary.

6. Claims should be clear and concise, but without the possibility of ambiguity or misinterpretation.

6.3.4 As noted above, no specific detail is provided in the PSyR with regard to the lower-level nuclear security claims that will be developed in the iterative GSR.

6.3.5 These lower-level claims will take account of and, thus, reflect:

1. Bounding (as necessary) the limited scope of the UK GDA security assessment, i.e. what is to be assessed during GDA and what would be covered by a nuclear site security plan (NSSP) for a nuclear licensed site.

2. Plant lifecycle stages and/or RR SMR operating conditions.

Arguments

6.3.6 Detailed arguments will be presented which will justify the security claims and point to the substantiating evidence.

6.3.7 In the main, these arguments will relate directly to the relevant claim or sub-claim; however, as necessary a single argument may support a connected set of claims and sub-claims.

Evidence

6.3.8 The evidence to substantiate the claims and arguments will be derived from a combination of relevant security and safety analyses and engineering design information. Several pieces of evidence may be required to support an argument; and a single piece of evidence may support more than one argument.

6.3.9 Nothing within this PSyR points towards the evidence that will be presented to substantiate the claims and arguments. This evidence will be produced as output from security analyses is integrated into engineering design.

7 Secure by Design

7.1 Introduction

7.1.1 This section sets out to indicate, in outline, how the following high-level nuclear security claim will be substantiated as the GDA nuclear security submission matures:

> **[NSy 1.0] Secure by Design** The protection from harm provided by the nuclear security arrangements will be risk informed, cognisant of and proportionate to the UK DBT and integrated into engineering design; through an approach that seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design. Alignment with the expectations of the relevant ONR Security Assessment Principles (SyAPs) will ensure that the nuclear security solution is adoptable by prospective future nuclear site licence holders.

7.1.2 This Level 1 claim will address the expectations of the relevant ONR Key Security Plan Principles (KSyPP), and Security Delivery Principles (SyDPs), which include (and are discussed further in this Section):

1. KSyPP 1, Secure by Design
2. KSyPP 2, The Threat
3. KSyPP 3, Graded Approach
4. KSyPP 4, Defence in Depth
5. KSyPP 5, Security Functional Categorisation and Classification
6. KSyPP 7, Codes and Standards
7. FSyP 5, Reliability, Resilience and Sustainability
8. SyDP 6.4, Vulnerability Assessments.

7.1.3 The intention is that the RR SMR will be Secure by Design; that is security will be embedded throughout the plant/site design rather than just an ‘add-on’ that has traditionally been the approach to nuclear security. In addition, this approach provides an opportunity to:

1. Innovate, where appropriate.
2. Consider the application of new technologies.
3. Consider new ways of operation.

7.1.4 Embedding all of E3S (and not just nuclear security) at the early system engineering requirements stage allows such to influence the design to reduce the risks presented by the RR SMR; and hence the need to rely on protective or mitigating measures.

7.1.5 Two of the enablers for successful and effective 'Secure by Design' are:

1. **Management Commitment to Securit**y – A visible commitment by management to security, to ensure that it receives the necessary priority and resource.

2. **Early Engagement** – Engage with security teams early when they can have the greatest input into the design of the nuclear facility; this is achieved primarily through involvement in design optioneering studies (see Reference [18]).

7.1.6 Management commitment to security is demonstrated by the inclusion of nuclear security as a critical component of the overall Engineering Management Plan.

7.1.7 Security Practitioners have been engaged with the design programme from the earliest opportunity. This has allowed them to contribute to the planning and governance of Rolls-Royce SMR, as well as to provide technical input to the engineering design of the RR SMR.

7.1.8 In terms of nuclear security, this ensures that nuclear security requirements receive equal priority to nuclear safety requirements. The security requirements should (as far as possible) be functional and traceable to the security objectives and principles.

7.1.9 It is important to recognise that Secure by Design is not solely the preserve of Security Practitioners; rather it requires a multi-disciplinary approach utilising a large range of technical and engineering skills. As such, security considerations will be threaded throughout the engineering design community and the design evolution.

7.1.10 A schematic illustrating the flow through the iterative Secure by Design process is shown on Figure 8.

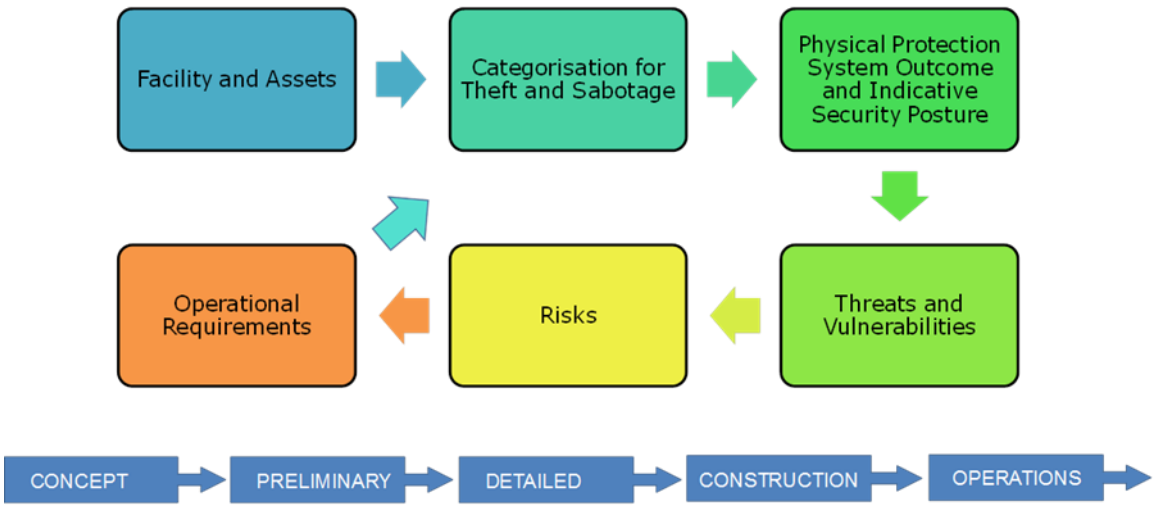


Figure 8 – Iterative Secure by Design Process Flow

7.1.11 To facilitate the various process which make up the overall Secure by Design process flow, it is necessary to have an appropriate understanding of the RR SMR and its constituent SSCs. A brief summary of the scope of design information that will be relevant to the various security analyses that will be undertaken is set out below.

7.1.12 The GDA Reference Designs that will be form the basis for Secure by Design are discussed in Paragraph 1.3.3.

7.2 Summary of Relevant Design Information

7.2.1 The policy adopted for the RR SMR is to achieve a standardised design and layout for the power station site.

7.2.2 The RR SMR comprises the following design areas (islands)[3];

1. **Reactor Island** which includes the systems that form the reactor, transfer and storage of new and used fuel, and any associated nuclear auxiliary systems. The purpose of Reactor Island is to use the heat from a controlled nuclear fission reaction to generate steam, which is then passed to the Turbine Island.

2. **Turbine Island** which provides the link between the Reactor Island where steam is generated, and the electrical connections where generated electricity is provided to the power grid. The primary SSCs in Turbine Island are the steam turbine and generator arrangement, where the thermal energy of steam is converted into electrical energy.

3. **Cooling Water Island** which provides the primary means of removing heat from the power station, passing it to the ultimate heat sink.

4. **Balance of Plant** which provides a range of ancillary functions to enable the other systems across the power station to achieve their functions, such as supply of demineralised water and chemicals.

5. **Electrical Control & Instrumentation** which includes systems relating to grid connection and intra-site electrical distribution, including emergency power supplies.

6. **Civil, Structural and Architectural** provides the physical structures which house, support and protect all other systems across the power station.

7.2.3 The relative locations of the Reactor Island and Turbine Island (together with other selected SSCs) are illustrated in Figure 9. Current design maturity includes for a separate 'off-site' Cooling Water Island.

7.2.4 Further details of the engineering design are provided in the RR SMR Design Overview Report (Reference [18]).

[3] Whilst some design areas (island) might be restricted to a single geographical location (e.g. Reactor Island), others might be more widespread (e.g. Balance of Plant).

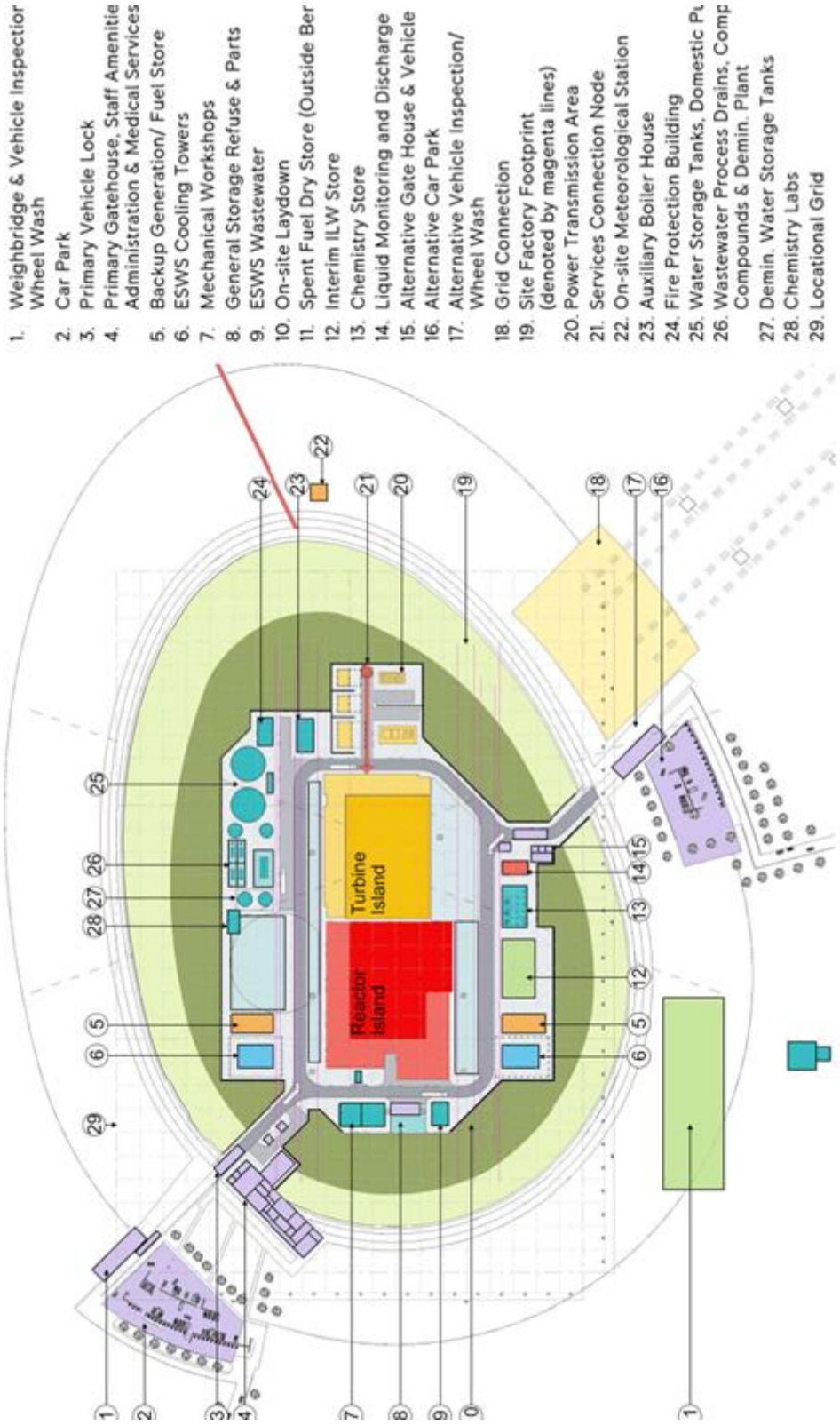


Figure 9 – Illustrative Site Layout

7.2.6 The three main areas and their supporting infrastructure (utilities, roads, drainage and security systems) are collectively referred to as the 'Power Unit'. The 'Power Unit' layout will be consistent for every site where the RR SMR is deployed globally. It will fix the positioning of the reactor island containment building and supporting safety systems buildings in relation to the spent fuel pool and its systems and the turbine island. It will also position the auxiliary buildings, water and fuel tanks and other buildings and facilities essential for day-to-day operations and emergency response within the reference site footprint.

7.2.7 The Reactor Island houses many of the targets for sabotage and/or theft, and therefore provides a focus around which both the PPS and CPS will be designed and constructed. This includes most of the NM and ORM that will be present on site; for example, both new and spent fuel rods and intermediate level wastes.

7.2.8 Many of the SSCs present on the Reactor Island are also potential targets for sabotage. These include (but are not limited to):

1. Reactor System, including pressure vessel, internals and fuel assemblies
2. Reactor Coolant System (RCS)
3. Duty Decay Heat Removal (DHR) Systems
4. Emergency DHR Systems, including Emergency Core Cooling System (ECCS)
5. Chemistry and Volume Control System (CVCS)
6. Reactor Plant Containment Systems
7. Reactor Island Control and Instrumentation (C&I) System
8. Reactor Reactivity Control Systems, including Control Rod Drive Mechanisms (CRDM)
9. Loss of Coolant Accident (LOCA) Protection Systems
10. Emergency Boron Injection (EBI) System
11. Refuelling System
12. Waste Treatment System (WTS).

7.2.9 SSCs requiring protection are less present within the Civil Structures (possible exceptions could include cooling water supply and radioactive waste storage facilities). However, many of the Civil Structures themselves will have a security function (in particular 'delay') or be required to house security systems such as detection systems.

7.2.10 Generally, SSCs located within the Turbine Island do not require protection as part of a nuclear security regime. Exceptions would be where the Turbine Island provides a pathway into the Reactor Island or where failure of an SSC could present a hazard to SSCs located on the Reactor Island.

7.2.11 The design of SSCs is undertaken through a systems engineering approach based on generating requirements (to address overarching RR SMR objectives and drivers) and developing a series of engineering solutions to achieve such. As such, the Reference Design for the RR SMR does not simply consider a single SMR configuration but rather families of designs that will be optimised and down-selected to ensure that the objectives are realised in the optimum way.

7.2.12 The range of operation states considered in engineering design and the nuclear safety case includes:

1. Build and commissioning requirements.
2. Power Operations including start-up and shutdown. This stage includes any Examination, Maintenance, Inspection and Testing (EMIT) activities undertaken whilst critical.
3. Shutdown operations intact, including transitions between power operation and shutdown, i.e. warm up and cool down. This stage includes non-intrusive examination and inspection.
4. Shutdown operations non-intact, including planned maintenance.
5. Refuelling operations.
6. In-service testing including physics tests.
7. Decommissioning and disposal requirements.

7.2.13 Secure by Design will need to be cognisant of all these operational states.

7.3 Secure by Design Principles

7.3.1 In designing security arrangements, the following SMR Secure by Design principles will be observed:

1. **Defence in Depth** – Defence in depth should ensure that there are no single points or perimeters of failure; and provide multiple opportunities to disrupt attack sequences.
2. **Graded Approach** – The application of a graded approach to the selection, implementation and assurance of security measures should ensure that the resources and degree of rigour is proportionate to the risk, and that measures are sustainable in the long-run.
3. **Full-life Design and Assurance** – Security systems should be designed for the full-life of the nuclear facility and have measures to assure their effectiveness throughout, i.e. SSC design should consider reliability, resilience and sustainability.
4. **Hierarchy of Security Controls** – The hierarchy of security controls promotes the elimination or reduction of security risk at source, before the application of dedicated security measures (see Figure 3).

5. **Integrated Engineering** – The integration of security delivery into engineering design evolution will ensure that the programme has the necessary skills and domain knowledge to achieve solutions with reduced inherent risk and integrated security features.

6. **Cross-Domain Risk Management** – Cross-domain risk management should be used to take advantage of safety, environmental or other measures that can also control security risks.

7. **Future Proof Against Emerging Threats** – The design of security systems should consider potential emerging threats and result in systems that are extensible and adaptable to counter as-yet unknown future threats.

7.3.2 These principles, when applied to the design of the power station, will facilitate solutions that minimise inherent security risk, incorporate security features directly into 'engineering' SSCs (i.e. integrated or intrinsic security measures), and ensure that effective security is maintained and assured throughout the life of the facility.

7.3.3 Secure by Design principles apply to both the PPS and CS&IA.

7.4 Threat Assessment

7.4.1 The UK DBT identifies malicious capabilities which confront the civil nuclear industry and provides assumptions about the composition and capabilities of terrorist groups and others posing a threat. The DBT is prepared based upon assessment undertaken by the Joint Terrorism Analysis Centre (JTAC) and issued by the Department for Business, Energy and Industrial Strategy (BEIS) in line with IAEA recommendations.

7.4.2 The DBT identifies the types of threat, and size and capability of the adversary force as the reference point for configuration of facility or design specific Vital Area Identification and Vulnerability Analysis. Guidance on the interpretation and use of the DBT is provide in ONR CNS-Tast-GD-11.4.2 (Reference [19]).

7.4.3 In addition to external malicious actors, it is essential that consideration is also afforded to 'insider' threat. The IAEA define the term 'insider' as 'one or more individuals with authorised access to nuclear facilities or NM in transport who could attempt unauthorised removal or sabotage, or who could aid an external adversary to do so'. The threat from an insider poses a unique problem due to the advantages they have over an adversary that does not have authorised access.

7.4.4 The DBT forms the basis for the design, evaluation and vulnerability assessment of protection systems to provide assurance that it will meet a defined security outcome.

7.4.5 All foreseeable threats (as defined in the UK DBT) will be identified and evidence provided that shows the RR SMR will have adequate protection in place to protect against them.

7.4.6 The ONR guidance also places an expectation on Dutyholders to set out how they will collect and analyse threat information. This aspect of KSyPP 2 is considered to be outside the proposed scope of the GSR for the RR SMR.

Target Identification

7.4.7 In determining the appropriate security measures for a PPS for the RR SMR it is necessary to identify the potential targets for sabotage and/or theft. This will be undertaken through the categorisation of the facility (and individual areas), against theft and the potential radiological consequences from sabotage (in line with guidance the Annexes to the ONR SyAPs.)

7.4.8 Target identification will commence as early as possible to ensure there is sufficient time to consider the opportunity to design out vulnerabilities or build in necessary security arrangements to mitigate the threat. Target identification will be reviewed throughout GDA (and through into site specific design and operation) to ensure security arrangement remain relevant and appropriate.

7.4.9 For protection against sabotage, target identification is linked with the potential for a resultant URC, as defined against dose thresholds set with the UK regulatory regime. Assessment of the consequences of sabotage should take into account not only direct sabotage of NM and ORM but also of SSCs that are necessary to maintain nuclear safety. Such SSCs deliver the safety functions of containment, cooling, and the control of criticality.

7.4.10 For protection against unauthorised removal or theft, the categorisation of radioactive materials ensures an appropriate relationship between the NM and ORM of concern and the requisite physical protection measures. Assessment to determine the categorisation for theft will also consider the aggregation of materials within an area.

7.4.11 A graded approach is adopted such that higher levels of protection are provided against events that could result in higher consequences; this in turn results in the provision of increased defence in depth for the most significant targets. This approach is in line with the expectations of KSyPP 3 - Graded Approach and KSyPP 4, Defence in Depth

7.4.12 A further discussion of categorisation for sabotage and theft is included in Section 8.

7.5 Vulnerability Assessment (Modelling)

7.5.1 It is an expectation of the ONR SyAPs that vulnerability assessments should be undertaken to validate the effectiveness of the PPS. The ONR provide guidance on the use of vulnerability assessment in CNS-TAST-GD-6.4 (Reference [20]).

7.5.2 Appropriate threat and vulnerability assessments are an essential input to the development of facility security requirements. By combining the findings of these assessments with information about the facility (e.g. site layout, and data network maps) into a model, security SMEs may:

1. Identify threat actor motivations, capabilities and likely goals.
2. Discover attack scenarios for combinations of threat actor, goal and capability.
3. Analyse the feasibility of attack scenarios.
4. Identify threat actions common to multiple attack scenarios.

5. Analyse the effectiveness of security measures in the modelled scenarios.

7.5.3 RR SMR will use vulnerability assessment throughout the design process, specifically as a means of validation that the proposed PPS will deliver the required Outcomes with sufficient confidence.

8 Physical Protection Solution

8.1 Introduction

8.1.1 This section sets out to indicate, in outline, how the following Level 1 nuclear security claims will be substantiated as the GSR matures:

1. **[NSy 2.0] Protection from Sabotage:** As far as is reasonably practicable, the Physical Protection System (PPS) will prevent malicious acts of sabotage which could result in Unacceptable Radiological Consequences. The PPS will deliver the security functions of 'Deter', 'Detect', 'Delay', 'Assess', 'Control of Access', and 'Insider Threat' – in order to address the relevant Design Basis Threat.

2. **[NSy 3.0] Protection from Theft:** As far as is reasonably practicable, the Physical Protection System (PPS) will prevent the theft of nuclear/radiological material or compromise of Sensitive Nuclear Information. The PPS will deliver the security functions of: 'Detect', 'Delay', 'Assess', 'Control of Access, and 'Insider Threat' - in order to address the relevant design basis threat.

8.1.2 Both of these claims relate principally to the design and delivery of a Physical Protection System (PPS) for the RR SMR. However, the output of the categorisation for both theft and sabotage will feed into the design of the CPS. The PPS will be delivered through the Secure by Design approach outlined in Section 7.

8.1.3 These higher-level claims will address the expectations of the relevant SyAPs, which include:

1. SyDP 6.1, Categorisation for Theft
2. SyDP 6.2, Categorisation for Sabotage
3. SyDP 6.3, Physical Protection System Design
4. KSyPP 5, Security Functional Categorisation and Classification
5. KSyPP 6.4, Codes and Standards.

8.1.4 The drivers behind the PPS are categorisation for sabotage and theft. These drivers will lead to zoning of the RR SMR site and the identification of the outcomes necessary for protection of targets within these zones. Typical zones include (in increasing order of protection) a limited access area, a protected area and a facility (which houses the protected targets).

8.1.5 Whilst to a large extent the measures to protect against theft and sabotage will be complimentary, we recognise that there will be some measures that are aimed primarily towards one or the other.

8.1.6 The PPS will be designed to deliver the expected outcomes and postures as defined in the Annexes to the SyAPs (Reference [2]); that is, protecting Category I to Category IV

quantities of NM/ORM against theft and the graded approach for the prevention of sabotage.

8.1.7 The PPS will be delivered through the incorporation of security functions (and eventually detailed specifications) into the engineering design. (Security functions are discussed in Sub-section 5.4). The delivery of these functions will make use of the Operation Requirements process (or something very similar).

8.1.8 Safety Case engineering uses a methodology to categorise safety functions (in terms of their importance to safety) and classify SSCs (in terms of their importance in delivering safety functions). This categorisation and classification result in appropriate design and quality assurance specifications, which in turn provide evidence to substantiate safety claims.

8.1.9 As part of the close alignment between the nuclear safety and security, a categorisation and categorisation scheme will be adopted for nuclear security (not just for the PPS but also with regard to CS&IA). We expect (but not exclusively the case) that there will be significant correspondence between safety and security; i.e. SSCs with a high safety classification are also likely to have a high security classification.

8.1.10 The classification of SSCs in terms of their importance in the delivery of security functions will ultimately lead to the identification and use of appropriate codes, standards and quality management processes. Such codes and standards are briefly discussed in this section.

8.1.11 An example engineering system flow that informs the PPS design process is illustrated in Figure 10. We are currently finalising the system for use with the RRS MR; this will be confirmed and presented as part of the GSR.

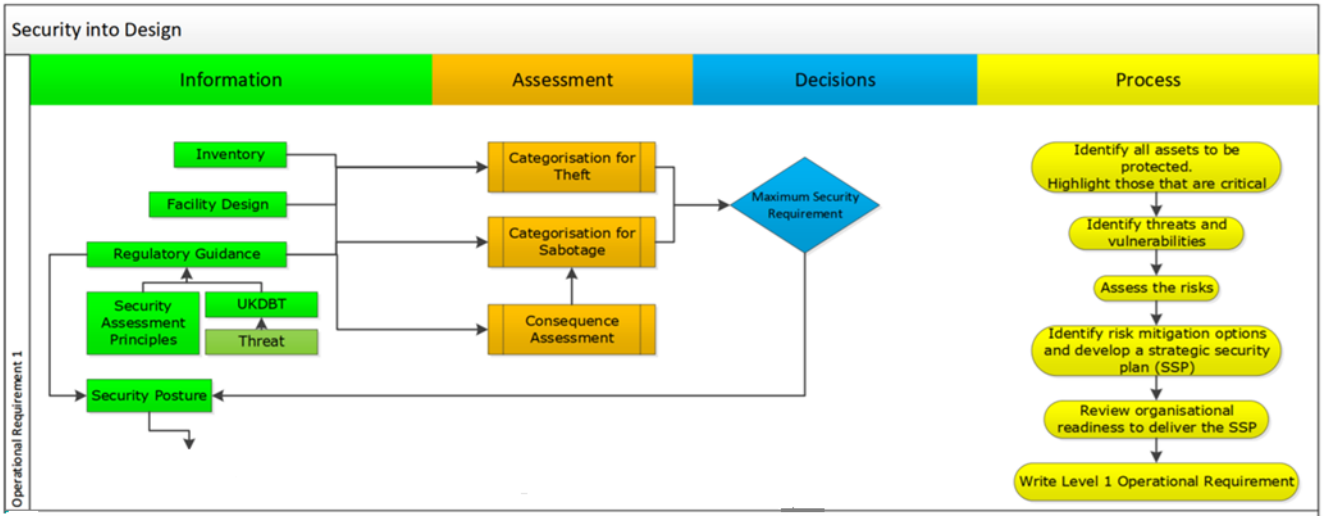


Figure 10 – Example Systematic Approach to Secure by Design

8.2 Categorisation for Sabotage (Vital Areas)

8.2.1 The CPPNM places an obligation on its member states to protect their nuclear facilities against sabotage. IAEA recommendations highlight that accepted good practice is to achieve this through a process of Vital Area Identification (VAI).

8.2.2 A VA is an area containing NM/ORM, or equipment, systems, structures or devices, the sabotage or failure of which, alone or in combination, through malevolent acts, could directly or indirectly result in a URC, thereby endangering people and the environment by exposure to radiation.

8.2.3 As outlined in the Unifying Purpose Statement (in SyAPs), dutyholders are responsible for the security arrangements to protect against sabotage; the expectations for which are further outlined through SyDP 6.2 – Categorisation for Sabotage. Annex B of the SyAPs (classified at Official-Sensitive) defines the radiological dose above which a URC would occur (for the UK); and further defines the categorisation of Vital Areas (VA) and High Consequence Vital Areas (HCVA) and the proportionate level of protection that is required for both. Additional guidance is provided in ONR TAG CNS-TAST-GD-6.2 Categorisation for Sabotage (Reference [21]).

8.2.4 The methodology whereby the RR SMR will be categorised for Sabotage (through a VAI) process is currently in development. This methodology will be based around the following:

1. Preparation Phase -

   a. Identification of the VAI Team – this will be a multidisciplinary team based around the core nuclear security team supplemented by SMEs covering nuclear safety, engineering design, layout and PWR operations.

   b. The Identification and Gathering of Input Data – this will include Policies and Principles, design and layout information, safety case information and supporting reports (e.g. fault schedules[4], HAZIDs, dose release fractions etc.).

2. VAI Process -

   a. Analysis of NM/ORM Inventory – taking into account its quantity location and physical form, the RR SMR inventory of NM and ORM will be analysed to determine whether (if unprotected/unmitigated) it is capable of producing a URC. That which is capable of resulting in a URC will be a candidate VA.

   b. Identification of IEMOs, Fault/Accident Sequences and SSCs – Initiating events of malicious intent (IEMOs) will be defined along with accidental/fault sequence which (if unmitigated/unprotected) could result in a URC. The SSCs in place to prevent the defined sequences developing (including safety systems) will be identified. These protective SSCs are identified as candidate VAs.

   c. Review of Sabotage Event Scenarios – Workshops will be held to review the capable sources of NM/ORM, the IEMOs, and protective SSCs to analyse whether (under a variety of operational states) the relevant sabotage scenarios are credible and could be realised; this will require significant input from relevant SMEs.

[4] VAI will consider potential initiating events that would be typically disregarded by safety assessment due to frequency (i.e. <1E-07 per year).

d. Assessment against UK DBT – The sabotage scenarios identified above will be assessed against the capability outlined in the UK DBT to determine if such would be capable of realising the scenario and resulting in a URC.

3. Identification and Categorisation of VA – Based on the sabotage scenarios that are realisable against the DBT, the associated NM/ORM and SSCs will be identified and categorised as either a VA or HCVA; and, the requirements for protection defined against the outcomes and postures in the SyAPs Annex.

8.2.5 The identification of VAs for the RR SMR will not wait until the design is mature, but will commence during (and support) engineering design. Initially, relatively informal (subjective) professional judgement will be made to identify candidate VAs and consider the potential for reduction of vulnerabilities. Thereafter, more formal (objective) methodologies will be developed and implement for use with a more mature design.

8.2.6 This early consideration of VAI is a significant enabler to the Secure by Design philosophy. Fully embedding security in the design phase allows for potential future security issues to be designed in such a way as to limit or even remove a potential risk, with the unified aim of achieving an optimal design across both safety and security.

8.2.7 As the design and associated safety case for the RR SMR plant will be developed in parallel with the implementation of the VAI process described above, a series of reviews will be programmed during this implementation period to consider the impact from any changes to the design and safety case.

8.2.8 As the engineering design matures, regular reviews of the categorised RR SMR VAs will be undertaken to assess the impact, if any, from:

1. Design modifications,
2. Changes to the safety case,
3. Any change to regulatory requirements,
4. Changes to the UK DBT.

8.3 Categorisation for Theft

8.3.1 The CPPNM (Reference [6]) also places an obligation its member states to protect their nuclear facilities against theft (i.e. unauthorised removal of NM and ORM for malicious purposes.

8.3.2 The CPPNM annexe is transposed into UK legislation through NISR. This requirement to protect against theft is incorporated into the ONR SyAPs through SyDP 6.1 - Categorisation for Theft; and, supplemented by further information in Annex A to the SyAPs (which is at Official Sensitive). Guidance is provided in ONR TAG CNS-TAST-GD-6.1, Categorisation for Theft (Reference [22]).

8.3.3 In the UK, categorisation of NM/ORM with regard to the quantities of (fissile) nuclides is as specified in Annex A of the SyAPs. This classification is different to that for sabotage (which is based on released radioactive dose). Categorisation for theft is

undertaken with regard to the potential for stolen NM/ORM to be used to produce a nuclear explosive device (NED), radiological dispersal device (RDD) or radiological exposure device (RED).

8.3.4 The NM/ORM on the RR SMR will be categorised accordingly against the tables in Annex A of the SyAPs. This characterisation will take into account the elements (comprising the NM/ORM), isotopic composition, and quantity. Consideration will also be given to the associated radiological dose and physical form of the NM/ORM, which can be an impediment to theft and/or its subsequent malicious use. Examples of the latter include the solidification and grouting of solid materials or the degree of dilution of fissile isotopes.

8.3.5 Categorisation for theft must also take into account aggregation of the total amount of NM in a facility, a group of buildings or a group of rooms – quantities of NM stored separately may not in themselves warrant a 'high' classification for theft, but could do so if they could all be stolen during a single attack.

8.3.6 As for VAI, undertaking classification for theft before a design is mature allows for the possibility of feedback into engineering design to reduce vulnerabilities to theft and ensure that an appropriate and proportionate security solution is derived and delivered through design.

8.3.7 Given the nature of the RR SMRRR-SMR, it is probable that the NM/ORM classified as needing the most protection from theft will also be identified as a Vital Area (VA) or High-Consequence VA (HCVA). Hence, there will need to be co-ordination in designing a PPS to protect against theft and sabotage; and, when specifying measure to protect against one, the impact on the protection of the other will be considered.

8.3.8 Likewise, there will be some overlap in protection of NM/ORM from theft (for malicious) purposes and the requirement for Safeguards (to prevent proliferation). Nevertheless, both require separate analysis of protection needs; and, protection of one may not be sufficient for protection of the other.

8.4 Design of Physical Protection System (PPS)

8.4.1 The required detail for the design of the PPS (to be included in the GSR) will be agreed between the ONR and Rolls-Royce SMR.

8.4.2 The Centre for the Protection of National Infrastructure (CPNI) is the UK Government's technical authority for protective security advice to UK national infrastructure. CPNI promotes the use of an Operational Requirement (OR) process. Where a suitable OR process has been used on UK civil nuclear projects, these projects have a significantly higher success rate and stakeholders are better engaged in the security measures implemented.

8.4.3 An OR process (or something similar) will be adopted to manage the development of a PPS and the integration of such into both the Secure by Design approach (see Section 7) and the overall engineering design of the PPS.

8.4.4 The use or an OR process or similar will be the primary method for defining functional requirements to those concerned with the design of the RR SMR. This offers a mechanism for security SMEs to articulate a desired capability or outcome that must

be achieved, so that the project can evidence that the design intent for Secure by Design.

8.4.5 Generally, this process is delivered in two parts:

1. **Operational Requirements Level 1, Security (OR1)** - which provides a strategic statement of security need and includes such detail as the assets to be protected, asset description, perceived threat, consequences of compromise, vulnerabilities and success criteria. This is expected, primarily, to lead to the identification of requirements for intrinsic security (see Paragraphs 5.5.1 to 5.5.7).

2. **Operational Requirements Level 2, Security (OR2)** – which follow on from OR1, and addresses security measures individually (fences, CCTV, access control, alarms etc.) and considers how individual solutions will combine to deliver an Integrated Protection Solution. This is expected, primarily, to lead to the identification of requirements for extrinsic security (see Paragraphs 5.5.1 to 5.5.7).

8.4.6 The use (at the relevant stages) of OR or similar will incorporate a security functional categorisation and classification scheme and identify appropriate codes and standards.

8.4.7 The use of OR 1 and OR 2 is illustrated on Figure 11.

8.4.8 The use of ORs will not be restricted to the design and specification of the PPS but may also be used in the development of the CPS.

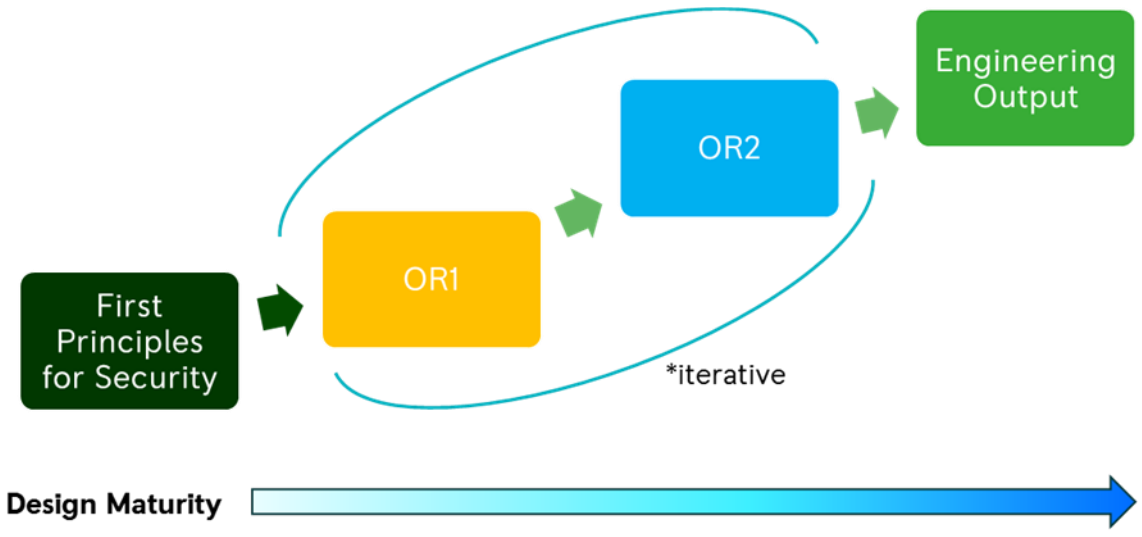


Figure 11 - Security Input to an Engineering Output

Security Functional Categorisation and Classification

8.4.9 Rolls-Royce SMR will develop a systematic approach to the identification and categorisation of security functions; and the subsequent classification of the SSCs and process/procedures which will deliver these functions. The functional categorisation

scheme will be linked in with the classifications for sabotage and theft and the associated expected security outcomes.

8.4.10 Set out below is a preliminary indication of the likely direction of travel in developing an appropriate categorisation and classification process.

8.4.11 It is an expectation of the ONR SyAPs (KSyPP 5) that SSCs, including software for instrumentation and control, are classified on the basis of their security significance, through a process of functional categorisation and classification (i.e. similar to that which is applied for nuclear safety purposes). The ONR expectations regarding functional categorisation and classification are set out further in in CNS-TAST-GD11.4.5 (Reference [23]).

8.4.12 Categorisation for both sabotage and theft will identify security outcomes and postures will feed into the design of a Physical Protection System (PPS) for the RR SMR.

8.4.13 A primary stage in the design of the PPS will include the definition of security functions for a variety of SSCs and supporting processes and procedures. These SSCs will likely fall into two main groups as follows:

1. SSCs whose primary purpose is other than the provision of a security measure (e.g. nuclear safety systems, primary cooling circuit etc.).

2. SSCs whose primary purpose is to provide a security measure (e.g. fences, alarms, CCTV etc.).

8.4.14 For the PPS, these security functions will be based around the functions of 'Deter', 'Detect', 'Delay', 'Assess', 'Control of Access', and 'Insider Threat' etc. (see Sub-section 5.4). As appropriate, these high-level security functions may be broken down further to aid in the development of the PPS; for example, 'Detect external threat at site boundary' and 'Detect external threat at entrance to Facility A'. The ONR SyAPs set an expectation that these security functions should be categorised in accordance with their security significance.

8.4.15 There will be a clear relationship between the required security outcomes and postures, and the categorisation of security functions and subsequent classification of SSCs. A possible simple security functional categorisation scheme (Reference [23]) could be based around the security postures, for example:

1. **Category A** - Security functions which delivers a 'fortified' posture.

2. **Category B** - Security functions which delivers a 'robust' posture.

3. **Category C** - Security functions which delivers a 'routine' posture.

4. **Not Categorised for Security.**

8.4.16 The categorisation assigned to each security function will be used to classify the structures, systems and components that deliver the function.

8.4.17 A possible classification scheme could be based around:

1. **Class 1, Principal Security Feature (PSyF)** - The most important security feature for countering the threat pathway being assessed.

2. **Class 2, Significant Security Feature (SSyF)** - Significant Security Features (SSyF) are second tier features, identified to achieve multiple layers of security where this is required.

3. **Class 3, Other Security Feature (OSyF)** - Other Security Features are identified as relevant good practice. They are explicitly identified to recognise their supporting role in achieving the holistic PPS against a specific threat pathway.

4. **Not Classified for Security.**

8.4.18 It is important that all SSCs are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification. The higher the classification the greater the quality assurance required for the SSC to ensure its availability and reliability in delivery of the security functions.

8.4.19 The proposed approach for the categorisation and classification of Security Functions intends to specify the role of any identified protective arrangements in their protection against both theft and sabotage, where appropriate, i.e. an element of the PPS may be a Principal Security Feature for the protection against theft, but a Significant Security Feature for protection against sabotage.

8.4.20 (Categorisation of security functions associated with software and control & instrumentation will also be undertaken – but is not discussed further in this Sub-section.)

Security Codes and Standards.

8.4.21 It is an expectation of the ONR SyAPs (KSyPP 7) that appropriate national or international codes and standards should be adopted for SSCs which deliver a security function. These codes and standards applied should reflect reliability requirements and be commensurate with their security classification. This also applies to CS&IA.

8.4.22 All SSCs will be designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their security classification. This is in line with the expectations of the following ONR SyAPs:

1. SyDP 5.1 – Reliability and Resilience

2. SyDP 5.2 – Examination, Inspection, Maintenance and Testing

3. SyDP 5.3 – Sustainability.

8.4.23 We will develop a systematic approach to the identification of appropriate codes and standards for SSCs/processes/procedures which fulfil a security function and deliver the appropriate security functional categorisation and SSC classification.

8.4.24 This approach will take into account existing national and international codes and standards as far as possible. If such standards are not wholly applicable, alternative standards may be developed taking into account such as operational experience SME judgment, of specific tests and analysis.

8.4.25 The adopted codes and standards will be justified against security requirements and functions.

8.5 Operation of the PPS

Concept of Operations

8.5.1 In conjunction with the design of the PPS a high-level Concept of Operations will be developed. This will demonstrate how the PPS should be operated to deliver the required security outcomes and identify any specific Human Factors which need to be taken into account.

8.5.2 The required detail for the Concept of Operations (to be included in the GSR) will be agreed between the ONR and Rolls-Royce SMR.

Policing and Guarding

8.5.3 In addition to a Concept of Operations, the GSR will also consider (in outline) requirements for policing and guarding.

8.5.4 Typically, general security duties as such as searching, monitoring alarms/CCTV and access control are delivered through use of (unarmed) security guards.

8.5.5 The Civil Nuclear Constabulary (CNC) has jurisdiction at designated nuclear sites, within 5km of those sites and wherever it needs to be to safeguard NM. The primary function of the CNC is to contribute to the security regime at those places to which it is deployed. This is through the provision of an armed response, that in combination with other security measures, is capable of denying unauthorised access to NM (which could result in theft or a URC).

8.5.6 ONR SyDP 9.1 (CNC Response Force) requires that Dutyholders should facilitate CNC deployment that is appropriate to achieve the required security outcome.

8.5.7 Rolls-Royce SMR understands and acknowledge the statutory responsibilities of the CNC and will liaise with CNC, as appropriate, during the development of the GDA security solution for the RR SMR.

9 Cyber Security & Information Assurance

9.1 Introduction

9.1.1 This section sets out to indicate, in outline, how the following Level 1 nuclear security claim will be substantiated as the GSR matures:

> **[NSy 4.0] Cyber Security & Information Assurance (CS&IA):** The focused application of CS&IA as part of a larger CPS will prevent malicious acts to all relevant digital assets (including OT and IT), or interruptions to services, that could foreseeably result in: Unacceptable Radiological Consequence, the theft of nuclear/ radiological material or the compromise of sensitive nuclear information. The CS&IA will deliver the functions of: 'Detect', 'Delay', 'Resist' and 'Recover' - in order to address the relevant design basis threat.

9.1.2 This higher-level claim will address the expectations of the following relevant SyAPs, which include:

1. SyDP 7.1, Effective Cyber and Information Risk Management
2. SyDP 7.2, Information Security
3. SyDP 7.3, Protection of Nuclear Technology and Operations
4. SyDP 7.4, Physical Protection of Information
5. SyDP 7.5, Preparation for and Response to Cyber Security Incidents
6. KSyPP 5, Security Functional Categorisation and Classification
7. KSyPP 6, Codes and Standards.

9.1.3 The most significant argument contributing to the substantiation of this claim will be the application of full-lifecycle cyber security standards to the full lifecycle of all computer-based systems within the GDA boundary. Secure by Design is the central tenet in the SMR Operational Technology Cyber Security Strategy (Reference [24]) which requires designs to demonstrate:

1. An integrated approach to safety and security, for example the inclusion of cyber security threats in Hazard and Operability Studies (HAZOPS).
2. The application of a formal risk management framework to the design, with risk management requirements incorporated into the design.
3. Self-protecting architectures that minimise the impact of compromise.
4. A graded approach to security that ensures that resources are applied where they are most effective, and that security measures are sustainable throughout the life of the power station.

5. A defence-in-depth approach that acts on all parts of the cyber-attack lifecycle to achieve resilient designs.

6. Co-ordination with supporting security functions, e.g. physical and personnel security, to ensure that risks are managed in a collaborative way.

7. A secure development lifecycle that encompasses the entire lifecycle of the equipment, from design to disposal.

9.1.4 ONR guidance on the approach to and requirements for CS&IA is provided in CNS-TAST-GD7.1, Effective Cyber and Information Management (Reference [25]).

9.2 Scope for CS&IA

9.2.1 The following systems are currently within the scope for CS&IA activities:

1. **Computer-Based Systems Important to Safety (CBSIS)** – These are computer-based systems used in processes or activities involving nuclear or other radioactive material, or upon which one or more claims will be made in a safety case. For the purposes of this strategy, CBSIS are further divided into the following sub-categories of systems -

   a. **Nuclear Instrumentation and Control (NI&C) Systems** – which are those systems conforming to BS EN 61513 Nuclear power plants – Instrumentation and control important to Safety – General requirements for systems (Reference [26]).

   b. **Electrical Instrumentation and Control (EI&C) Systems** – which are those systems conforming to BS EN 61850-3 Communication networks and systems for power utility automation – Part 3: General requirements (Reference [27]).

   c. **Electrical, Electronic or Programmable Electronic (E/E/PE) Safety-Related Systems (SRS)** - which are those systems conforming to BS EN 61508-1 Functional safety of electrical/electronic/programmable electronic safety related systems - Part 1: General requirements (References [28]).

2. **Computer-Based Security Systems (CBSy)** – These are the sensors and systems that will be identified in the nuclear site security plan as being functionally important in delivering or maintaining a site security function.

3. **Information Technology (IT)** – The RR SMR will make use of a significant number of digital technologies to realise operational efficiencies throughout its life. Traditionally, OT and IT systems have been very separate, with the former being primarily occupied with control and safety functions where information integrity is the priority, and the latter being occupied with information management activities where confidentiality (particularly of SNI) leads. Digital vastly increases the number and complexity of the interfaces between these worlds; where IT security may previously have been left to the site operator, for RR SMR the distinction between IT and OT is not as well defined.

4. **Other systems** – There are likely to be non-safety and non-security related systems that are necessary in maintaining the availability of the power station to produce electricity, or are indirectly relied upon by CBSIS, CBSy or production

systems. These will be identified by the likely impact of their failure on safety, security or production.

9.3 Operational Technology

9.3.1 The objectives of the CS&IA activities within the OT domain are:

1. **To assure nuclear and conventional safety** – The CS&IA arrangements for the RR SMR will meet our ethical and legal obligations to protect society from potential harm arising from licenced site activities.

2. **To prevent malicious acts which could result in Unacceptable Radiological Consequences** – The CS&IA arrangements will prevent unauthorised access to CBSIS (which could facilitate sabotage of nuclear processes), or CBSy (which could facilitate the theft NM/ORM).

3. **To prevent compromise of sensitive information** – Sensitive information relating to the security, design and operation of the RR SMR could aid the execution of malicious acts such as theft and sabotage.

4. **Protect the availability of generation** – The economic sustainability of the power station is dependent on its ability to generate energy. Extended or frequent disruption of production could threaten the economic sustainability of the power station and have wider impacts on the stability of the electrical grid.

9.3.2 Requirements relating to these objectives have been included in the functional requirements of the power station and regular contact by the SMR cyber security function with the relevant stakeholders is maintained to ensure that technical work progresses towards achieving these goals.

9.4 Information Technology

9.4.1 The objectives of the CS&IA activities with the IT domain, relating to the design of the power station are:

1. **To prevent compromise of sensitive information** – Digital systems will decrease the amount of logical and physical space between sensitive information and external systems; therefore, additional care will be taken to ensure that any operational gains offered by these systems will be realised without compromising the confidentiality of sensitive information.

2. **To assure nuclear and conventional safety** – Outputs from digital systems will be used in operational refinements and decision making; therefore, the provenance and integrity of information in the IT domain will be managed to ensure that downstream systems and processes are provided with data that has a level of trust consummate with its intended application.

9.4.2 Regular contact by the SMR cyber security function with the relevant stakeholders is maintained to ensure that technical work progresses towards achieving these goals.

10 Summary

10.1 Summary of PSyR

10.1.1 This PSyR seeks to demonstrate that Rolls-Royce SMR has the requisite understanding and experience of the UK regulatory regime and of the expectations of the ONR for a GDA nuclear security submission. Furthermore, this PSyR sets out our proposed approach to (and scope) of the GSR that will be the main document within our GDA security submission.

10.1.2 Presented within this PSyR (Section 6) are the fundamental and higher-level security claims that will form the backbone of the GSR. The Level 1 claims are:

1. [NSy 1.0] Secure by Design
2. [NSy 2.0] Protection from Sabotage
3. [NSy 3.0] Protection from Theft
4. [NSy 4.0] Cyber Security & Information Assurance (CS&IA).

10.1.3 This PSyR sets out the Security Objectives and Design Principals (see Section 4) that will drive a systems engineering approach to the development of the security arrangements for the RR SMR. These arrangements will be substantiated within the GSR using a 'claims-argument-evidence' approach.

10.1.4 As emphasised throughout this PSyR, the commitment to build security into the design of the RR SMR has been in-place from the start of Rolls-Royce SMR, and security professionals have provided advice and input from the concept design phase onwards.

10.1.5 Essentially, this Secure by Design approach has (and continues to) comprised two main (but nonetheless inter connected) threads:

1. **The integration of security into engineering design** – that is to seek to address security vulnerabilities as early as possible in the design process; and (ideally) remove or reduce such (as far as is practicable taking into account operational and safety requirements and constraints).
2. **The design of security SSCs** – that is to utilise a systems engineering approach to design of SSCs the primary purpose of which is to provide the security functions such as delay (e.g. fences and other barriers) detect (e.g. CCTV, alarms etc.).

10.1.6 Both of these threads seek to adopt the SMR security principles (see Sub-section 5.3) and will demonstrate how the expectations of the ONR with respect to KSyPP1 will be addressed. Likewise, both of these threads will contribute to the successful delivery of a security solution for the RR SMR (GDA Design) which will be 'fit for purpose' and proportionate to threat and risk.

10.2 Development of GSR

10.2.1 The development and substantiation of the security arrangements will be set out in a Generic Security Report (GSR).

10.2.2 The GSR will represent the Security Case for the generic RR SMR. The GSR will be presented in a 'claims-arguments-evidence' approach. The GSR will be supported by appropriate topic reports and other evidential documents.

10.2.3 Subsequent construction and operation of a RR SMR will require further development of a site-specific Security Case and ultimately (in the UK) of Nuclear Site Security Plan (NSSP).

11 References

[1] Office for Nuclear Regulation, ONR-GDA-GD-006 (Revision 0), “New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties,” October 2019.

[2] Office for Nuclear Regulation, “Security Assessment Principles for the Civil Nuclear Industry (Version 1),” March 2022.

[3] Rolls-Royce SMR, SMR0000520, Issue 05, “Engineering Management Plan for RR SMR,” April 2022.

[4] Rolls-Royce, EDNS01000613500, Issue 2, “SMR Generic Design Assessment Boundary Document,” June 2020.

[5] Office for Nuclear Regulation, “Classification Policy for the Civil Nuclear Industry, Version 8.01,” November 2017.

[6] International Atomic Energy Agency, “Convention on the Physical Protection of Nuclear Material,” October 1979.

[7] International Atomic Energy Agency, “Amendment to The Convention on the Physical Protection of Nuclear Material,” July 2002.

[8] International Atomic Energy Agency, “Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear SEcurity Series No 16,” 2013.

[9] International Atomic Energy Agency, IAEA Nuclear Security Series No. 27-G, “Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5),” 2018.

[10] International Atomic Energy Agency, IAEA Nuclear Security Series No. 16, “Identification of Vital Areas at Nuclear Facilities,” 2013.

[11] Office for Nuclear Regulation, “Safety Assessment Principles for Nuclear Facilities, Revision1,” January 2020.

[12] Office for Nuclear Regulation, CNS-TAST-GD11.1 (Issue 1.2), “CNS-TAST-GD11.1, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs,” May 2021.

[13] Office for Nuclear Regulation, ONR-GDA-GD-007 (Revision 0), “ New Nuclear Power Plants: Generic Design Assessment Technical Guidance,” May 2019.

[14] Rolls-Royce SMR, TBC/Draft, “Environment, Safety, Security and Safeguards (E3S) Management Manual,” May 2022.

[15] Rolls-Royce SMR, SMR0001175 July 2022, “Guidance on E3S Document Categorisation,” July 2022.

[16] Rolls-Royce SMR, SMR0000627, Issue 1, “E3S Case Development Strategy,” May 2022.

[17] Rolls-Royce, EDNS010000659017, Issue 003, “UK SMR Enviroment, Safety, Security and Safeguarding Principles,” December, 2020.

[18] Rolls-Royce, SMR0000594, Issue 1, “RR SMR Design Overview Report,” June 2022.

[19] Office for Nuclear Regulation, CNS-TAST-GD-11.4.2, Issue 1, “The Threat,” April 2022.

[20] Office for Nuclear Regulation, CNS-TAST-GD-6.4 (Issue 1.1), “Vulnerability Assessment,” April 2022.

[21] Office for Nuclear Regulation, CNS-TAST-GD-6.2 (IRevision 1), “Categorisation for Sabotage,” April 2020.

[22] Office for Nuclear Regulation, CNS-TAST-GD-6.1 (Revision 1), “Categorisation for Theft,” April 2020.

[23] Office for Nuclear Regulation, CNS-TAST-GD11.4.5, Issue 1, “Functional Categorisation and Classification of Security Structures, Systems and Components,” April 2022.

[24] Rolls-Royce, EDNS01000505017/001, “Rolls-Royce Small Modular Reactor Operational Technology Cyber Security Strategy,” April 2017.

[25] Office for Nuclear Regulation, CNS-TAST-GD-7.1 (Revision 1), “Effective Cyber and Information Management,” March 2020.

[26] British Standards Institute, BS IEC 61513:2011, “Nuclear Power Plants - Instrumentation and controls important to safety - General requirements for systems”.

[27] British Standards Institute, BS EN61850-3, “Communication networks and systems for power utility automation, Part 3: General requirements,” August 2014.

[28] British Standards Institute, BS EN61508-1, “Functional safety of electrical/electronic/programmable safety-related systems, Part 1: General Requirements,” June 2010.

12 Acronyms and Abbreviations

ALARP	As Low As Reasonably Practicable
ASCE	Assurance and Safety Case Environment
BAT	Best Available Techniques
BEIS	[The Department of] Business, Energy and Industrial Strategy
C&I	Control and Instrumentation
CAE	Claims-Argument-Evidence (approach)
CBSIS	Computer-Based Systems Important to Safety
CBSy	Computer-Based Security Systems
CCTV	Closed-Circuit Television
CNC	Civil Nuclear Constabulary
CPNI	Centre for the Protection of National Infrastructure
CPPNM	(IAEA) Convention on the Physical Protection of Nuclear Material
CPS	Cyber Protection System
CRDM	Control Rod Drive Mechanism
CS&IA	Cyber Security & Information Assurance
CVCS	Chemistry and Volume Control System
DBT	Design Basis Threat
DD	Developed Design
DHR	Decay Heat Removal
DOORS	Dynamic Object-Orientated Requirements System
DR	Definition Review
DSEAC	Design, Safety and Environment Advisory Committee
E3S	Environment, Safety, Security & Safeguards
EA	Environment Agency
EBI	Emergency Boron Injection
ECCS	Emergency Core Cooling System
E/E/PE	Electrical, Electronic or Programmable Electronic
EI&C	Electrical Instrumentation and Control
EMIT	Examination, Maintenance, Inspection and Testing

EPRI	Electric Power Research Institute
FCD	Full Concept Design
FSyP	Fundamental Security Principle (from ONR SyAPs)
GDA	Generic Design Assessment
GSR	Generic Security Report (for GDA)
HAZOPS	Hazard and Operability Studies
HCVA	High Consequence Vital Area
IAEA	International Atomic Energy Agency
IC	Intelligent Customer
ICSANT	International Convention for the Suppression of Acts of Nuclear Terrorism
IE	Initiating Event
IEMO	Initiating Event of Malicious Origin
IMS	Integrated Management System
ISMS	Information Security Management System
ITA	Independent Technical Assessment
IT	Information Technology
ICSANT	United Nations International Convention for the Suppression of Acts of Nuclear Terrorism
JTAC	Joint Terrorism Analysis Centre
KSyPP	Key Security Plan Principle (from ONR SyAPs)
LOCA	Loss of Coolant Accident
MDSL	Master Document Submission List
NED	Nuclear Explosive Device
NIA	Nuclear Installations Act 1965
NI&C	Nuclear Instrumentation and Control
NISR	The Nuclear Industries Security Regulations 2003 (as amended)

NM	Nuclear Material
NRW	Natural Resources Wales
NSL	Nuclear Site Licence
NSSP	Nuclear Site Security Plan
NSy	Nuclear Security
ONR	Office for Nuclear Regulation
ONR CNSS	Office for Nuclear Regulation, Civil Nuclear Security & Safeguards
OR	Operational Requirement
ORM	Other Radioactive Material
OSyF	Other Security Function
OT	Operational Technology
PCD	Preliminary Concept Design
PCS	Pressure Control System
PIE	Postulated Initiating Event(s)
PPS	Physical Protection System
PSyF	Principal Security Function
PSyR	Preliminary Security Report (for GDA)
RASyP	Regulatory Assessment of Security Plans (from ONR SyAPs)
RCS	Reactor Coolant System
RDD	Radiological Dispersion Device
RED	Radiological Exposure Device
RIO	Regulatory Interface Office
Rolls-Royce SMR	Rolls-Royce SMR Ltd (the Requesting Party)
RP	(GDA) Requesting Party
RR SMR	The (engineering design of the) Rolls-Royce Small Modular Reactor
SAPs	(ONR) Safety Assessment Principles
SEPA	Scottish Environment Protection Agency
SLIS	Small Leak injection System
SME	Subject Matter Expert
SNI	Sensitive Nuclear Information

SRS	Safety Related System
SSCs	Structures, Systems & Components
SSyF	Significant Security Function
SSyP	(UK) SMR Security Principle
SyAPs	(ONR) Security Assessment Principles
SyBD	Secure by Design
SyDPs	Security Delivery Principles (from ONR SyAPs)
TAG	(ONR) Technical Assessment Guide
TIG	(ONR) Technical Inspection Guide
TOR	Terms of Reference
URC	Unacceptable Radioactive Consequence
VA	Vital Area
VAI	Vital Area Identification
WTS	Waste Treatment System