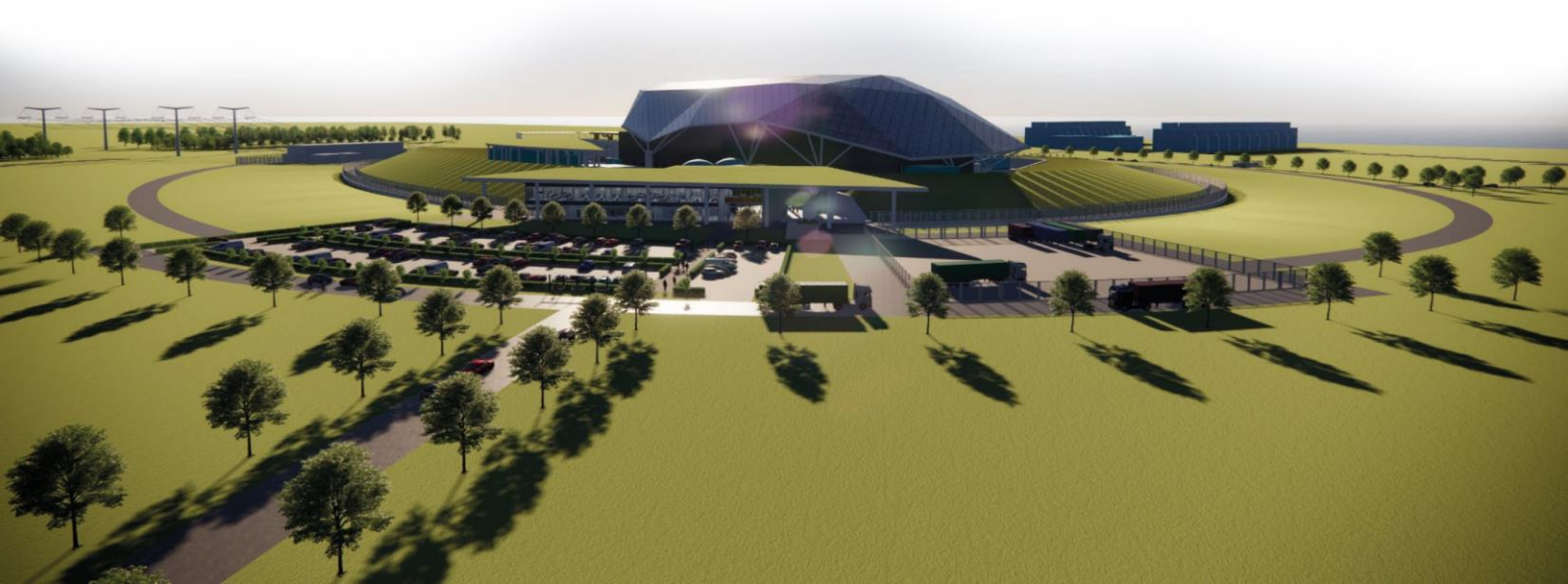
Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 32: Generic Security Report



Record of Change

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First Issue of E3S Case
March 2024	2	Issue	Revision of site, plant, and environmental information at Reference Design 7, aligned to Design Reference Point 1 Also reflects updated content from the E3S Case Development and Management Arrangements (SMR0000627) and E3S Requirements and Analysis Arrangements (SMR0009132)
May 2024	3	Issue	Updated to correct revision history status at Issue 2. Chapter changes include: • Revision to wording of Fundamental Nuclear Security Claim (section 32.2.3.1) • Clarification on purpose of ONR SyAPs (section 32.2.5.31) • Clarification that the security analyses are consequence driven (section 32.3.1.3) • Revision of wording of security functions (section 32.3.4) • Inclusion of personnel security in list of security arrangements (section 32.3.4) • Revision of wording to claim 32.1.2 (section 32.5 and Table 32.14-1) • Conformation that all of the individual security analyses could be relevant to an individual SSC • Replacement of 'Recognised' by 'Relevant' good practice • Clarification over the scope of cyber protection system (section 32.7.1) • Clarification that the development of the Integrated Security Solution will include identification of Outcomes and Postures (section32.7.8) • Clarification that requirements for the physical and cyber security systems are based on analysis against threat interpretation (section 32.9.7) • Clarification that power and space are required by both civilian and armed-response guard forces (section 32.9.7) • Additional detail for how arguments and evidence presented meet generic E3s case objective (section 32.12.3) Also, minor template/editorial updates for clarification and overall E3S Case consistency

Executive Summary

This Generic Security Report (GSR) summarises the Nuclear Security Case for the Rolls-Royce Limited Small Modular Reactor (RR SMR). The security case forms part of an integrated Environment, Safety, Security and Safeguards (E3S) Case for the RR SMR. The GSR forms Chapter 32 of the E3S Case.

The Nuclear Security Case is constructed around five main themes:

- Secure by Design
- Protection from Theft
- Cyber Security & Information Assurance
- Protection from Sabotage
- Integrated Security Solution.

Rolls-Royce SMR Limited has adopted a Secure by Design (SbyD) approach to the development of a security solution, with security embedded (wherever possible) within the engineering design.

The primary function of the SbyD approach is to link the security analyses to the development of the integrated security solution (ISS) and link the development of the security case with engineering design.

At a high-level, the outputs from SbyD (in conjunction with the development of the ISS) can be summarised as:

- Influence (informal) and requirements (formal) on the engineering structure, systems and components, which reduce security risk and vulnerabilities
- High-level requirements for the design of physical and cyber protection system measures to address residual security risk.

This issue of the GSR provides an overview of the SbyD approach together with the methodologies for the security analyses that underpin SbyD. These methodologies identify the security outcomes and posture that an Integrated Security Solution (ISS) for the RR SMR must meet.

Future issues of the GSR will summarise the outcomes and postures identified and the subsequent development of an ISS for the RR SMR.

The primary objective of the ISS is to provide a future Operator/Dutyholder/Permit holder with a full understanding of the security solution for the RR SMR and how it has been developed. By understanding how the ISS has been developed, why security functions and measures have been selected and their links to the E3S, it is possible to derive a security plan for an operational RR SMR.

Contents

Tables

Figures

32.1 Introduction to Chapter

32.1.1 Introduction

The RR SMR has a fundamental objective 'to protect people and the environment from harm'. The Environment, Safety, Security & Safeguards (E3S) Case is being developed to provide the overall justification that the fundamental objective can be achieved at all lifecycle stages of the power station and demonstrate that risks can be reduced to As Low As Reasonably Practicable (ALARP), applying Best Available Techniques (BAT), and ensuring Secure-by-Design (SbyD) and Safeguards-by-Design.

Rolls-Royce SMR Limited are using a claims, arguments, evidence (CAE) approach to structure the overall E3S Case in the demonstration of ALARP, BAT and SbyD. A more detailed summary of the approach to and benefits of the integrated E3S Case is provided in the E3S Case Version 2, Tier 1, Chapter 1: Introduction [1].

The E3S Case comprises a series of 33 chapters that cover the broad scope of Environment, Safety, Security and Safeguards. A full list of the chapters of the E3S case is provided in the E3S Case Version 2, Tier 1, Chapter 1: Introduction [1].

32.1.2 Objective of the Generic Security Report

The Generic Security Report (GSR) forms Chapter 32 of the overall E3S Case. For convenience and to aid the reader, the part of the E3S Case covered within Chapter 32 is referred to in this Chapter as the Nuclear Security Case.

This version of the GSR summarises the current development of the Nuclear Security Case, with reference to other supporting documents or other sources of information. An indication is also given of the contents of future issues.

In accordance with the overall E3S Case, the Nuclear Security Case is presented through a CAE approach. The E3S Case is hierarchical in structural, comprising of three tiers (Tier 1, Tier 2 and Tier 3) of documentation [1].

The final issue of the Nuclear Security Case should be sufficient to form the basis of the Nuclear Site Security Plan (NSSP) to be developed by a future Nuclear Site Licence (NSL) holder in the UK. Key in achieving this objective is an understanding of the Integrated Security Solution (ISS) for the RR SMR.

32.1.3 Background

Rolls-Royce SMR Limited is developing a nuclear power station design based around Small Modular Reactor (SMR) technology, known as the Rolls-Royce SMR (RR SMR). The RR SMR design programme is a phased design cycle, which commenced in May 2016 and aims to deploy the First of a Fleet (FOAF) RR SMR in the early 2030s.

A detailed summary of design and the engineering framework is provided in of the E3S Case, Version 2, Tier 1, Chapter 1: Introduction [1], in the following sections:

- Section 1.3, Engineering Framework
- Section 1.4, Site Layout
- Section 1.5 General Plant Description.

The RR SMR is designed as a modular and standardised power station product. This means that each RR SMR is substantively the same as the others; so far as is possible within the constraints of site-specific geography. The RR SMR has a planned lifetime of approximately 60 years, with refuelling and maintenance required periodically. A brief introduction to the design is included in this sub-section to provide background and aid the reader.

The RR SMR comprises the following design areas (islands):

- Reactor Island
- Turbine Island
- Cooling Water Island
- Balance of Plant
- Electrical Control & Instrumentation
- Civil, Structural and Architectural.

The relative locations of the Reactor Island and Turbine Island (together with other selected SSCs) at Reference Design (RD) 7 / Design Reference Point (RPD) 1 stage are illustrated in Figure 32.1-1. Current design maturity includes for a separate 'off-site' Cooling Water Island.

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 (see Section 1.3 of E3S Case Version 2, Tier 1, Chapter 1 [1].

Monitoring and control of the RR SMR is centralised within the Main Control Room (MCR), located within Reactor Island. If the MCR is uninhabitable (e.g., due to fire), then the operators can transfer to the Supplementary Control Room (SCR). The RR SMR also includes an on-site Emergency Control Centre (ECC) and associated facilities for managing events. An off-site ECC will also be provided; this may be shared between power stations dependent on location. A Security Control Centre (SyCC) and additional access control points provide the ability to monitor and control site access.

A key criterion for the RR SMR is a compact and modular design. This challenges the traditional approaches to nuclear security, which typically rely on open ground and large structures to detect, delay and respond to adversaries.

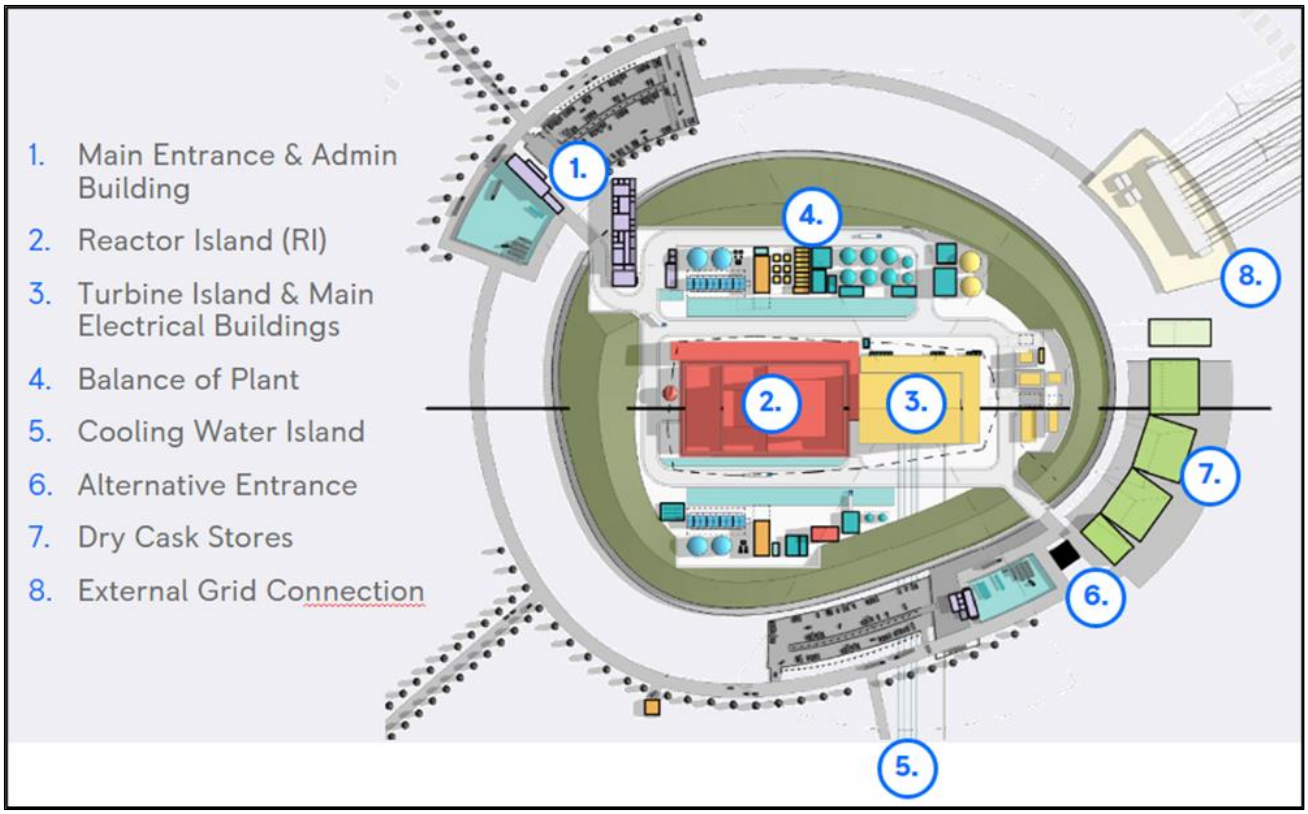


Figure 32.1-1: RR SMR General Site Layout (at RD7/RDP1)

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 are designed and constructed. Many of the civil structures will have a security function (for example delay and/or control of access) or be required to house security systems such as detection systems.

Relevant design information is also be summarised in Tier 2 and Tier 3 of the Nuclear Security Case, together with further reference to detailed engineering information. The security solution takes account of all operational states (see Section 1.5 of E3S Case Version 2, Tier 1, Chapter 1 [1]).

The design is currently subject to a Generic Design Assessment (GDA) by the Office for Nuclear Regulation (ONR). The extent of the design that is within scope for the GDA is set out in the scope and boundary document [2].

32.1.4 Scope of the Generic Security Report

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

The philosophy behind the Nuclear Security Case 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 a result of malicious acts.

Rolls-Royce SMR Limited has chosen to adopt a SbyD approach to the development of a security solution, with security embedded (wherever possible) within the engineering design. Traditional

security measures are incorporated into the RR SMR to address the residual risk following the application of SbyD.

The Nuclear Security Case is constructed around five main themes:

- Secure by Design (see Section 32.5)
- Protection from Theft (see Section 32.6)
- Cyber Security & Information Assurance (see Section 32.7)
- Protection from Sabotage (see Section 32.8
- Integrated Security Solution (see Section 32.9).

This issue of the GSR provides an overview of the SbyD approach together with the methodologies for the security analyses that underpin SbyD. The security analyses have been trialled and potential learning and improvements identified. These methodologies are now being applied to the relevant structure, systems and components (SSCs) which make up the RR SMR.

These methodologies identify the requirements for an Integrated Security Solution for the RR SMR. These are captured within the Rolls-Royce SMR Limited requirements management database [3].

Future issues of the GSR will summarise the identified requirements and the subsequent development of an ISS for the RR SMR.

32.1.5 Structure of This Chapter

- Section 32.1, Introduction – This section discusses the purpose and introduces the contents of the document.
- Section 32.2, Nuclear Security Case – This section introduces the scope of the Nuclear Security Case and its structure.
- Section 32.3, Security Objectives and Principles – This section provides an overview of the security objective and SbyD principles which have been adopted to aid the design of the security solution.
- Section 32.4, Threat Interpretation – This section provides an overview of the interpretation of the UK Design Basis Threat (DBT) for use in assessing security risk to the RR SMR.
- Section 32.5, Secure by Design – This section introduces the SbyD approach that has been adopted for the RR SMR.
- Section 32.6, Categorisation for Theft – This section introduces a methodology for Categorisation for Theft (CFT) and how it is applied. Future issues will summarise the Security Outcomes and Postures identified by the methodology.
- Section 32.7, Cyber Security – This section introduces a methodology for the assessment of cyber security risks and how it is applied. Future issues will summarise the Security Outcomes and Postures identified by the methodology.

- Section 32.8, Vital Area Identification and Categorisation – This section introduces a methodology for Vital Area Identification and Categorisation (VAI&C) and how it is be applied. Future issues will summarise the Security Outcomes and Postures identified by the methodology.

- Section 32.9, Integrated Security Solution – This section sets out the approach to the development of an Integrated Security Solution (ISS) for the RR SMR. Future issues will summarise what the ISS comprises.

- Section 32.10, Integration of Nuclear Security with other E3S Topic Areas – This section summarises the interaction between nuclear safety and other E3S topic areas.

- Section 32.11, Development of a Site Security Plan – This section introduces an overview of how the ISS can be used to develop a site-specific security plan for an operational RR SMR.

- Section 32.12, Conclusions – Future issues will provide a summary of the assumptions, commitments, and requirements arising from the Security Case and which are critical to the successful implementation of the ISS.

32.1.6 Limitations and Exclusions

32.1.6.1 Limitations

This issue of the GSR was crafted to reflect the security case information available at the time of publication. The security case continues to mature, and future iterations of the GSR will capture changes.

The current scope of the security case primarily addresses the operating phase of a nuclear power station. The current scope does not cover security during manufacture, construction, or commissioning lifecycle phases.

This issue of GSR sets out the development of 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, in future issues of the security case.

The current scope of the security case assumes that the generic RR SMR site is not located adjacent to other nuclear licensed facilities. On this basis, this GSR does 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.

32.1.6.2 Exclusions

This GSR does not cover the topic of Nuclear Safeguards. Nuclear Safeguards is covered within E3S Case Version 2, Tier 1, Chapter 33: Safeguards [4].

This GSR 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 outside the scope of the security assessment at GDA.

32.1.7 Security Classification for this Document

None of the information contained within this document is Sensitive Nuclear Information (SNI), as defined in accordance with the Classification Policy for the Civil Nuclear Industry [5].

The intention is that main body of future issues of this report should, if possible, remain unclassified. To this end, the use of classified annexes is proposed. These annexes would be referenced within the main text, but contained within a separate classified document that can be handled and managed appropriately.

32.2 Nuclear Security Case

32.2.1 Introduction

The Rolls-Royce SMR E3S Case demonstrates that the E3S fundamental objective for the RR SMR, 'to protect people and the environment from harm', can be achieved at all lifecycle stages of the power station. As noted in Section 1, the part of the E3S Case covering nuclear security, is referred to in this Chapter 32 as the Nuclear Security Case.

The Nuclear Security Case is presented as a hierarchy of documents that describe the conceptual security design, underpinned by risk-based analysis drawn from Relevant Good Practice (RGP). The security case summarises the nuclear material (NM), other radiological materials (ORM), vital areas (VAs) and operational technology (OT) that need to be protected within an ISS. The ISS outlines how security risks are designed out and residual risks are mitigated by designing in security features.

The Nuclear Security Case must present evidence that the proposed design is likely to comply with Nuclear Industries Security Regulations 2003 (NISR 2003) [6]. It must also demonstrate that regulatory expectations within the ONR Security Assessment Principles (SyAPs) [7] can be met.

32.2.2 E3S Case

Full details of the development, aims and scope of the E3S Case are included as E3S Case Version 2, Tier 1, Chapter 1: Introduction of the case [1]. A brief summary is included in this sub-section to aid the readers of Chapter 32.

The E3S Case comprises a series of 33 chapters that cover the broad scope of Environment, Safety, Security and Safeguards.

The RR SMR E3S Case is hierarchical, comprising the following 'tiers' of information:

- Tier 1: an entry point to the E3S Case that presents the decomposition of claims with a proportionate, overarching summary of the arguments and evidence in lower tiers of the E3S Case
- Tier 2: the first level of underpinning information, comprising a set of summary documents that present the detailed E3S requirements, arguments and / or evidence that underpin the lowest decomposed claims in the Tier 1 report, and also signpost out to the detailed evidence on Tier 3
- Tier 3: the detailed evidence for different aspects of the E3S Case to underpin claims, supporting the arguments or evidence contained within Tier 2 documents.

The fundamental E3S claim is decomposed into a set of top-level claims aligned to each Tier 1 chapter of the E3S Case. Each top-level chapter claim is then decomposed into supporting sub-claims, with decomposition to a level such that the lowest level of sub-claim is of sufficient detail to point to arguments and/or evidence within Tier 2.

The RR SMR is a developing design that is not based on an existing reference plant. As the design progresses through the concept design stage and into detail design, a generic E3S Case is developed based on a set of generic site characteristics and design parameters known as the

Generic Site Envelope [8]. The development of the generic E3S Case is illustrated in Figure 32.2-1, aligned to programme maturity stages and engineering RDs with an indication of which revision is submitted at the end of each step of the regulatory Generic Design Assessment (GDA) process.

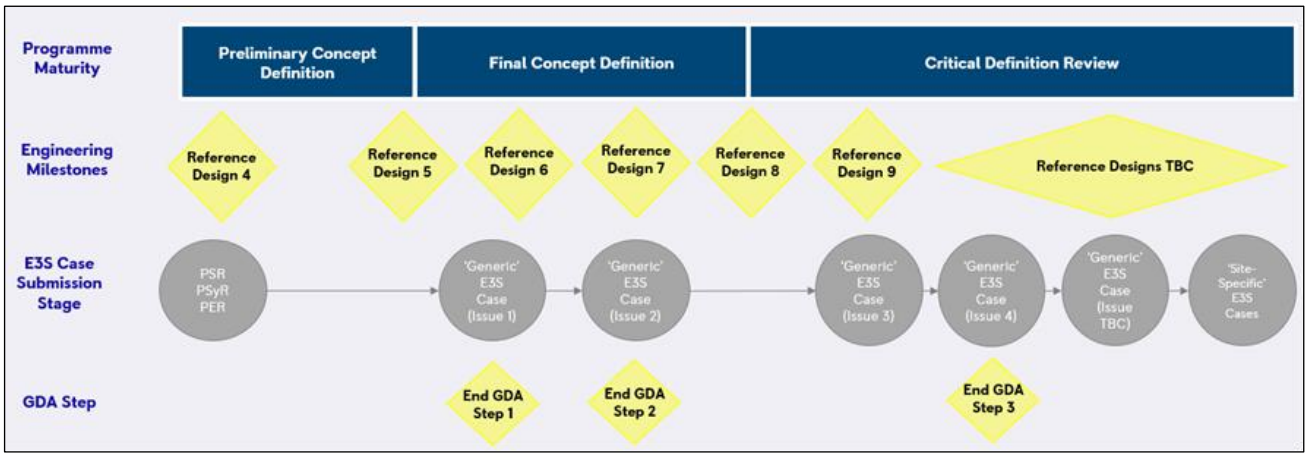


Figure 32.2-1: Generic E3S Case Evolution

32.2.3 Nuclear Security Case

As for the overall E3S Case, the Nuclear Security Case is developed initially with reference to relevant UK regulation and guidance. As such, the case provides the basis for the subsequent development of a Nuclear Site Security Plan (NSSP) for an operational RR SMR in the UK[1]. Nevertheless, reference is made to international regulations and guidance and the security case should also provide a suitable basis for the development of a nuclear security plan for an RR SMR located overseas.

As noted in Section 1, the E3S Case is using a CAE and presented in a tiered structure; this also applies to the Nuclear Security case. All of the claims and sub-claims presented or referenced in this Chapter represent the current roadmap for the security case. These claims and sub-claims are subject to revision and/or addition as the security case develops.

32.2.3.1 Fundamental Nuclear Security Claim

The top-level claim for the Nuclear Security Case is:

[E3S Claim 32.0] Fundamental Nuclear Security Claim - The design of the 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 is achieved through the adoption of internationally accepted standards and Relevant Good Practice (RGP) as promoted by the International Atomic Energy Agency (IAEA); and will be compliant with the relevant national regulatory regime.

The Rolls-Royce SMR Limited nuclear security objectives (see Section 32.3) reflect both: the moral obligation to protect people and the environment from harm (both conventional and nuclear) and there are commercial imperatives on the security of the RR SMR which are drivers of engineering

[1] This excludes Scotland and Northern Island.

design (for example, availability of electricity generation, protection of intellectual property rights). These two sets of objectives are not necessarily exclusive.

The ISS for the RR SMR is developed to achieve these security objectives through the application of the Rolls-Royce SMR Limited SbyD Principles [9].

32.2.3.2 Level 1 Nuclear Security Sub-claims

The Fundamental Security Claim is decomposed into a set of five high-level (Level 1) sub-claims, which reflect the primary focus of a nuclear security regime to satisfy regulatory obligations (as outlined in the ONR SyAPs [7].

These five Level 1 Security sub-claims are as follows:

[E3S Claim 32.1] Secure by Design: Security risk inherent in the design has been minimised through the application of secure by design principles and a credible secure by design methodology that integrates security considerations into the design process and security measures into SSCs, in a way that is consistent with the operational intent of the RR SMR, and before the application of dedicated security controls.

[E3S Claim 32.2] Protection from Theft: Material at risk of theft has been identified through the application of a Categorisation for Theft Methodology. Security measures have been identified, and applied in a Graded Approach, to minimise the risk of theft. These security measures form part of an Integrated Security Solution (ISS) for the generic RR SMR.

[E3S Claim 32.3] Cyber Security & Information Assurance (CS&IA): The risks to all digital assets (including Operational Technology [OT] and Information Technology [IT]) associated with the generic RR SMR shall be reduced to an acceptable level through the use of CS&IA as part of a larger Cyber Protection System (CPS), within an Integrated Security Solution (ISS). Risks to be mitigated include sabotage resulting in an Unacceptable Radiological Consequence, the theft of nuclear/radiological materials, the compromise of sensitive nuclear information, as well as lesser consequences such as plant interruptions, industrial hazards and lesser radiological consequences.

[E3S Claim 32.4] Protection from Sabotage: The design basis threat of the sabotage of nuclear material or other radioactive material which could result in Unacceptable Radiological Consequence will be managed through the application of a Vital Area Identification and Categorisation (VAI&C) Methodology to identify requirements for proportionate security measures. These security measures will form part of an Integrated Security Solution (ISS) for the generic RR SMR.

[E3S Claim 32.5] The Integrated Security Solution (ISS) has been developed for the generic RR SMR. The ISS provides future Operators with a full understanding of the security solution and how it has been developed; and provides the basis for the subsequent development of a security plan for an operational RR SMR which will both meet regulatory expectations for nuclear security and address the commercial risk appetite of the Operator.

This approach to the development of the GSR partly mirrors that for nuclear safety, which is focussed on ‘control of reactivity’, ‘control of fuel temperature’, ‘confinement of radioactive material’ and ‘control of radiation exposure’.

32.2.3.3 Level 2 and 3 Nuclear Security Sub-claims

The Level 1 sub-claims have been decomposed into sets of supporting Level 2 sub-claims and, in some cases, Level 3 sub-claims. The intention of which is to link these lower-level sub-claims with the various pieces of evidence which, when taken together, demonstrate that the Fundamental Nuclear Security Claim has been met.

The lower-level claims are tabulated in the following appendices:

- [E3S Claim 32.1] - Secure by Design (in Appendix A in Section 32.14)
- [E3S Claim 32.2] - Protection from Theft (in Appendix B in Section 32.15)
- [E3S Claim 32.3] - Cyber Security & Information Assurance (in Appendix C in Section 32.16)
- [E3S Claim 32.4] - Protection from Sabotage (in Appendix D in Section 32.17)
- [E3S Claim 32.5] - Integrated Security Solution (in Appendix E in Section 32.18).

Whilst these high-level claims are based primarily around regulatory compliance, the underlying sub-claims also address commercial imperatives.

32.2.4 Structure of Nuclear Security Case

In accordance with the overall structure of the E3S Case, the Nuclear Security Case is presented in a tiered structure and based around the CAE approach.

This Tier 1 GSR is supported by a series of Tier 2 'topic reports' one for each of the topic areas covered by the Level 1 Nuclear Security sub-claims. Each of these Tier 2 documents sets out the sub-claims relevant to the 'topic' and summarise the substantiating evidence (with reference to the detailed Tier 3 evidence).

Each of the Tier 2 documents is underpinned by numerous Tier 3 evidence. This evidence will be wide ranging, including outputs from security analyses, engineering design data and layout information. The Tier 3 information is contained in reports, spreadsheets, drawings or outputs from digital databases.

Tier 2 and 3 documents are referenced as appropriate in the later sections of this Chapter.

32.2.5 Regulatory Framework for the Nuclear Security Case

As stated in the Fundamental Security Objective, the overarching objective of a nuclear security case is to protect people and the environment from the consequences of malicious actions. The achievement of this objective is the subject a both international and national regulatory regimes, to which a nuclear security case must demonstrate compliance.

This sub-section presents a brief overview of the main sources of regulatory requirements, associated regulatory guidance and other Relevant Good Practice that are relevant to this Chapter. This sub-section is not intended to be an exhaustive discussion.

32.2.5.1 International Regulation and Guidance

The UK is obliged to establish and maintain a legislative framework to govern the physical protection of NM, ORM and Sensitive Nuclear Information (SNI) in accordance with the following international conventions:

- The Convention on the Physical Protection of Nuclear Material (CPPNM) - The CPPNM [10] places obligations on signatory states to protect nuclear facilities, and material in peaceful domestic use, in storage and in transit.

- The United Nations International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) [11] which requires signatories to make every effort to adopt appropriate measures to ensure the protection of radioactive material.

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

With regard to nuclear security matters, relevant IAEA guidance includes:

- 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 [12]

- Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), Implementing Guide No. 27-G, 2018 [13]

- Identification of Vital Areas at Nuclear Facilities, Technical Guidance Reference Manual, Technical Guidance No. 16, 2013 [14].

32.2.5.2 United Kingdom

The principal pieces of UK legislation which regulate the Civil Nuclear Industry in the UK are:

- The Nuclear Installation Act (NIA) 1965, under which, the construction and operation of a nuclear power station (in the UK) requires a Nuclear Site Licence (NSL).

- The Nuclear Industries Security Regulations (NISR) 2003 (as amended) [6] which 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 a NSSP.

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. As part of its role, the ONR provides guidance to Dutyholders (NSL holders and others subject to regulation by the ONR) on the UK expectations for nuclear security.

This guidance represents the ONR view of good practice, which the ONR expects modern facilities to satisfy their overall intent. 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.

The ONR guidance includes that set out in the overarching ONR SyAPs [7] and supporting Technical Assessment Guides (TAGs).

32.2.5.3 Security Assessment Principles

The primary purpose of the SyAPs [7] is to provide the ONR with a framework for making consistent regulatory judgements on the adequacy of security arrangements. Although it is not their primary purpose, they 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.

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) [15].

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.

The SyAPs are presented in four sets:

- 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:
    - 'Strategic Enablers' (FSyP 1 to 5), which are focused on the creation of the right conditions to support high reliability security arrangements (ie they are concerned with enabling the delivery of an effective security strategy)
    - 'Secure Operations' (FSyP 6 to 10), which are focused on the implementation and maintenance of nuclear security (ie they are concerned with the delivery of secure operations)
- Security Delivery Principles (SyDP) – these support the Fundamental Security Principles and set out the specific outcomes that deliver an effective nuclear security regime
- Key Security Plan Principles (KSyPP) – these are principles which can be applied across the breadth of the FSyPs and SyDPs
- Regulatory Assessment of Security Plans (RASyP) – these are principles which set out the foundations for effective security plans.

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 GSR.

The SyAPs are accompanied by a series of Annexes [16] which include a series of 'postures' and 'outcomes' to inform the requirements for a physical protection System (PPS) and cyber security and information assurance (CS&IA). The SyAPs annexes are classified at Official-Sensitive: SNI.

32.2.5.4 ONR CNSS Technical Assessment Guides (TAGs)

ONR CNSS has developed a series of nuclear security 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.

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 are consulted as appropriate.

The main TAGs relevant to the content of this Chapter include:

- CNS-TAST-GD-6.1, Categorisation for Theft [17]]
- CNS-TAST-GD-6.2, Categorisation for Sabotage [18]
- CNS-TAST -GD-7.1, Effective Cyber and Information Risk Management [19]
- CNS-TAST-GD-11.4.1, Secure by Design [20]
- CNS-TAST-GD-11.4.2, The Threat [21]
- CNS-TAST-GD-11.4.5, Functional Categorisation and Classification of Security Structures, Systems and Components [22].

A full list of relevant TAGs is not included here. Rather, other relevant TAGs are referenced as appropriate elsewhere in this Chapter and throughout the RR SMR Nuclear Security Case as a whole.

32.3 Security Objectives and Principles

32.3.1 Introduction

The RR SMR is being developed through a systems engineering approach which includes all of the E3S disciplines as key stakeholders supporting the design development and engineering processes.

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

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 help achieve these objectives.

As highlighted throughout this Chapter, 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.

32.3.1.1 Fundamental E3S Objective

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

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'

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

32.3.1.2 Potential Sources of Harm

When considering the potential sources of harm associated with a nuclear power station, these fall into two groups:

- Nuclear – that is harm that can result from exposure to ionising radiation
- Conventional – all other source of harm, for example physical and chemotoxic.

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.

32.3.1.3 Risk Informed

In alignment with the approach in the UK, the RR SMR has adopted a risk-informed approach to nuclear security rather than a strictly risk-based one. This approach is consequence driven rather than by the probability of a threat manifesting itself. 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.

The security arrangements 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 is taken in protecting against these design basis risks.

32.3.2 Security Objectives – Nuclear and Conventional

One of the commercial objectives of Rolls-Royce SMR Limited is that it is 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.

The nuclear security objectives for the RR SMR set the high-level security requirements that inform engineering design decisions.

The Rolls-Royce SMR Limited 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).

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.

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:

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

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

- To prevent compromise of SNI – 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.

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

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

- 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.

- 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.

32.3.3 Security by Design Principles

The Rolls-Royce SMR Limited has defined a series of E3S Fundamental Principles [23]. These principles provide a design framework whereby the RR SMR is evaluated and developed to ensure that it will operate safely and securely.

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.

The design and operation of the RR SMR should ensure SbyD whereby vulnerabilities are eliminated or reduced by design rather than secured or mitigated with add-on security measures. Where inherent security is not reasonably practicable, security measures should be provided (these could be either passive or active).

The security objectives for the RR SMR are delivered through the application of the SbyD principles which are set out below. The derivation of these principles is in line with the wider development of E3S principles [23] and consistent with the expectations of the ONR SyAPs [7].

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

In designing security arrangements, the following SMR Secure by Design principles are observed:

- 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.

- 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.

- 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.

Hierarchy of Security Controls – The hierarchy of security controls promotes the elimination or reduction of security risk at source, before the application of passive and then active security measures (see

- Figure 32.3-1).

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

- 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.

- 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.

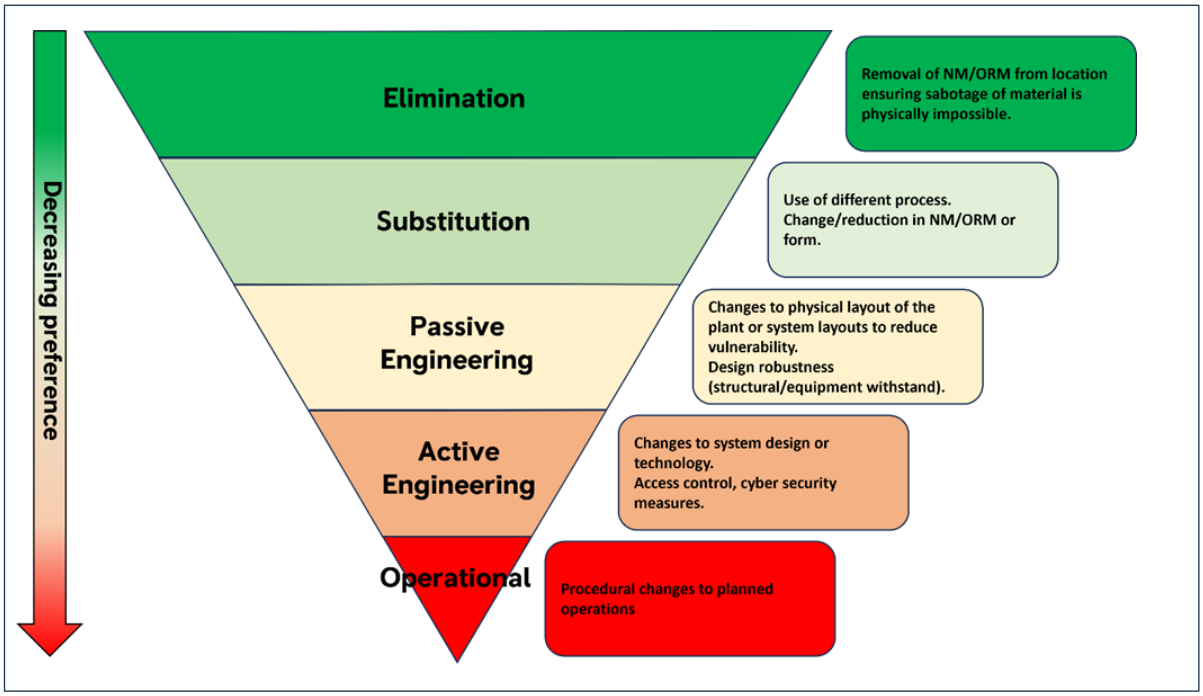


Figure 32.3-1: Hierarchy of Security Controls

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

32.3.4 Security Functions

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

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

The security functions that are required of the PPS are:

- Deter – to discourage a potential threat actor from doing something by instilling doubt or fear of the consequences
- Delay – provide a sufficiently robust design to permit a responding force to achieve the required outcome
- Detect – systems and arrangements to alert a responding force to a potentially malicious or unauthorised act
- Assess - systems and arrangements to enable a responding force to determine if an attack is underway and allow them to direct an effective response
- Control of Access – systems and arrangements to ensure only authorised personnel can again access to restricted areas and protected assets
- Insider Mitigation – process and arrangements to determine if a person is acting suspiciously or out of character, to allow immediate action to be taken or an investigation to be launched.

The security functions that are required of the CPS are:

- Identify – catalogues the software and hardware assets, identifies any potential vulnerabilities, determines the governance arrangements, commercial and regulatory environment, and identifies relevant threats and cyber security risks
- Protect – implements appropriate measures to defend information systems and mitigate the risks identified in the cyber security risk assessment
- Detect – provides a timely indication of a potential cyber security incident
- Respond - contains cyber security incidents, e.g. by restricting connectivity to critical systems, bringing systems to safe states where this is appropriate, communicating the incident to responders and collecting evidence
- Recover – restores systems and data, restores functionality and confidence in system performance, and prevents reoccurrence.

Security functions are provided 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. Security functions are recorded in the requirements management database as (functional) requirements.

Examples of the security arrangements that can deliver some of these security functions are illustrated on Figure 32.3-2. In practice, a combination of security function types is needed to achieve defence in depth.

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 and integrated security solution and in so doing deliver an overall deterrence.

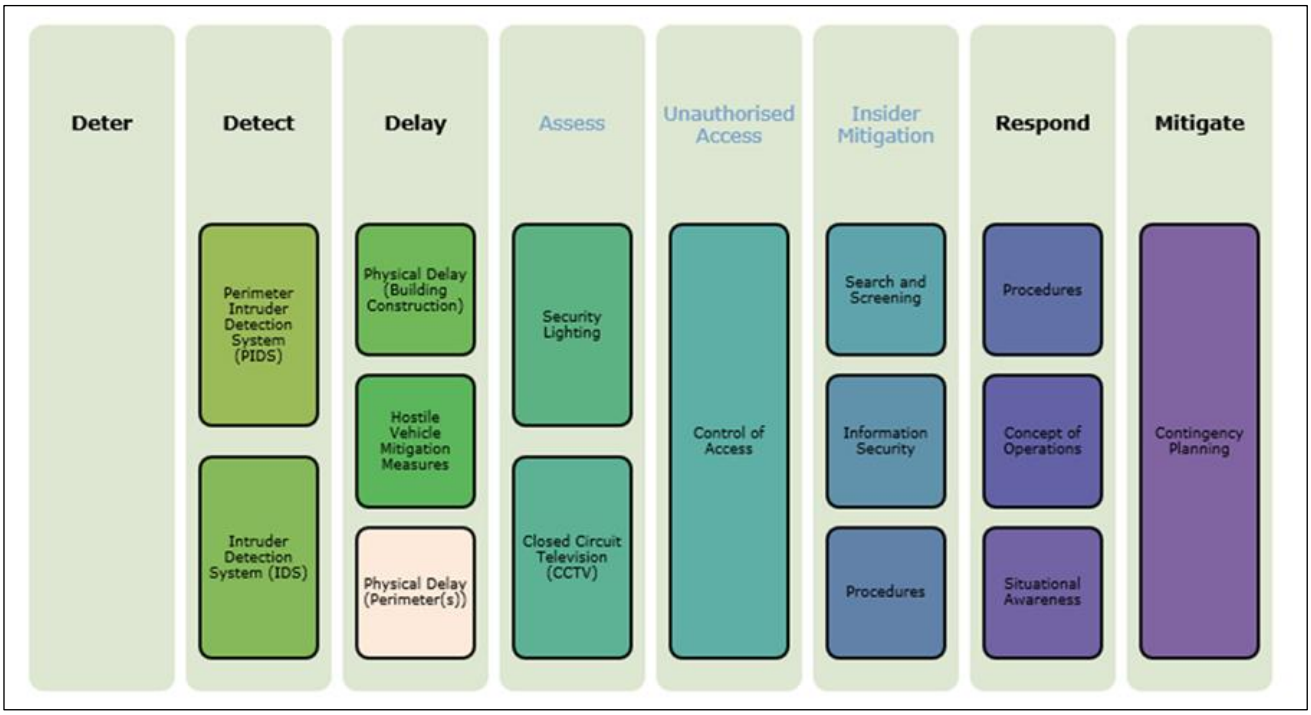


Figure 32.3-2: Layered Arrangements of Security Functions

32.3.5 Integration of Nuclear Security into the RR SMR Design

32.3.5.1 Engineering Design

Traditionally, reduction in nuclear security risk has been achieved through applying dedicated security controls (extrinsic security) to a fully developed nuclear power station. 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.

Rolls-Royce SMR Limited has adopted a SbyD approach whereby:

- Preliminary (high-level) security requirements are identified at the concept stage of design and integrated into the overall engineering requirements process.
- The appropriate security arrangements are developed alongside the maturing engineering design and supported by the integration of more detailed requirements.

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

The design of extrinsic security arrangements also follows a requirements-led SbyD process whereby the chosen options are substantiated rather than just what has been used previously.

The successful application of a SbyD approach:

- Encourages efforts to reduce security risk at source, before considering the effect of a security protection system

- Adopts a system-level, or systems engineering, approach to the design of nuclear security arrangements
- Engineers features into the design of the SSCs that have security functionality
- Encompasses the entire lifecycle of the facility.

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 to ensure the integration of security functionality and requirements into the design of the RR SMR.

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.

At a high (concept) level, these security requirements relate to the Fundamental Security Principle (see sub-section 32.3.3) 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 leads 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.

Each SSC has its own dedicated modules within the requirements management database [3], covering requirements specification, design definitions, and verification strategies. The database enables links between these modules, providing traceability of design information.

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

32.3.5.2 Nuclear Safety

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 might also satisfy the requirements for nuclear security.

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 is concerned with initiating events of malicious origin (IEMO) which could intentionally trigger accident fault sequences and the loss of safety functions (criticality, cooling, confinement).

Whilst a common approach is preferable, on some occasions a common solution is 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 is generally given to nuclear safety concerns, with the security risk addressed by extrinsic arrangements.

Given this complementary relationship between safety and security, the SbyD approach seeks to bring the nuclear safety and nuclear security cases into close alignment; to the extent that a large part of the evidence that substantiates both submissions are shared.

The integration between the nuclear safety and nuclear security is perhaps best illustrated in the process for identifying vital areas. 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 a URC.

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).

In addition to recognising the similarities between nuclear safety and security, it is also 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.

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.

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.

32.4 Threat Interpretation

32.4.1 Introduction

The threat to be applied to the Security Case is mostly defined by the UK Government in the UK Design Basis Threat (DBT) document. The threat is based on an adversary that acts in a deliberate, planned fashion that is not amenable to a numerical risk estimation.

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 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 provided in ONR CNS-Tast-GD-11.4.2 [21].

Threat intelligence comes in a variety of forms. For physical and personnel security, this includes from the National Protective Security Authority quarterly briefings [24]. It is recognised that the threat definition for the cyber threat is not complete as the threat capability in this subject develops at an ever-increasing rate. Therefore, the cyber threat capability is supplemented with further advice from other Government Agencies such as the National Cyber Security Centre (NCSC).

Rolls-Royce SMR has produced a Threat Interpretation document [25], based upon the UK DBT, guidance from the ONR and other Government agencies. This Threat Interpretation is used as the basis for all security assessment.

32.4.1.1 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to threat interpretation.

More detailed CAE is presented in the most recent issue of the following Tier 2 report:

- Rolls-Royce SMR: Interpretation of Design Basis Threat (DBT) for the Generic Rolls-Royce SMR [25]

This Tier 2 document will reference other relevant Tier 3 sources of evidence.

32.4.2 Claims Addressed

The top-level claim for the Nuclear Security Case is:

[E3S Claim 32.0] Fundamental Nuclear Security Claim - The design of the 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 top-level claim is supported by Level 1 and 2 sub-claims, the intention of which is to link them with the various pieces of evidence which, when taken together, demonstrate that the claim and sub-claims.

Threat Interpretation is cross-cutting and therefore sub-claims associated with it are spread across multiple areas.

32.4.2.1 Sub-Claims Associated with Secure by Design

[32.1.1.2] The capabilities of threat actors and the ways in which they might exploit the design to cause a radiological release, steal nuclear material or compromise sensitive nuclear information are understood, and the design incorporates integrated security measures to defend against these capabilities where this is practical and consistent with the operational intent of the RR SMR.

[32.1.3] The capabilities and likely goals of threat actors are understood.

[32.1.4.1] The postulated scenarios have been screened to eliminate any scenarios for which threat actors do not possess the necessary capability.

32.4.2.2 Sub-claim Associated with Protection from Theft

Although the Threat Interpretation applies to all aspects of design and operations no specific claims have been made associated with protection from theft.

32.4.2.3 Sub-claims associated with Cyber Security

[32.3.2] Cyber security risks shall be assessed using threat-based risk assessment process utilising the RR SMR Threat Interpretation to provide a graded security approach based on the system consequences.

[32.3.3] Cyber security control sets shall be implemented to reduce cyber security risks to an acceptable level, in a graded approach based on the consequences of system compromise and the skill of the threat actor.

32.4.2.4 Sub-claims associated with Protection from Sabotage

[32.4.1.5] Rolls-Royce SMR has assessed the credibility of the applied design basis threat to result in an URC through sabotage of the Targets (NM/ORM and preventative/protective/mitigating SSCs) as a result of physical, cyber or blended attacks.

32.4.2.5 Sub-claims associated with the Integrated Security Solution (ISS)

Although the Threat Interpretation applies to all aspects of design and operations no specific claims have been made (as yet) in association with the ISS.

32.4.3 Overview of Threat Interpretation

32.4.3.1 Limitations on Current Analysis Work

Methodologies, trial analysis and reports generated by Rolls-Royce SMR Limited to date have (with the exception of the Secure-by-Design analysis [26] and the Threat Interpretation [25] documents) been generated with commercial classifications only. This was done to aid their production by maximising the ability to share documentation. To enable this, the information provided in US Code of Federal Regulations (CFR) Title 10, Part 73.1 (10 CFR 73.1) [27]was used as a surrogate DBT for the physical threat.

This has limitations, and Rolls-Royce SMR Limited recognised that for future deployment of the methodologies and the application of SbyD, CfT, VAI&C and Cyber Security Risk Assessment (CSRA), will need to be undertaken using the full UK DBT.

32.4.3.2 Threat Assessment

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.

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

The ONR guidance also places an expectation on Dutyholders (for an operational RR SMR) to set out how they will collect and analyse threat information.

32.4.3.3 Target Identification

In determining the appropriate security measures for a PPS and a Cyber CPS for the RR SMR it is necessary to identify the potential targets for sabotage and/or theft. This is undertaken through the categorisation of the facility (and individual areas) for theft of NM/ORM and the potential radiological consequences from sabotage, in line with guidance the Annexes to the ONR SyAPs [16].

Target identification commences 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 is reviewed throughout GDA, and through into site specific design and operation, to ensure security arrangements remain relevant and appropriate.

For protection against sabotage, target identification is linked with the potential for an event with a resultant URC. For the UK this is defined against dose thresholds set within the ONR SyAPs Annexes [16]. Assessment of the consequences of sabotage takes into account not only direct sabotage of NM and ORM but also of Safety Significant Components (SSCs) that are necessary to maintain nuclear safety. Such SSCs deliver the safety functions of containment, cooling, and the control of criticality.

32.5 Secure by Design

32.5.1 Introduction

Rolls-Royce SMR Limited has adopted a SbyD approach to the development of a security solution, with security embedded (wherever possible) within the engineering design. To this end, security considerations have been an input from the beginning of the concept design stage of the RR SMR (starting in 2016).

The expectation is that such an approach delivers a more effective and robust ISS compared to a traditional solution applied through the addition of layers of security on top of a finalised design. This in turn should result in a reduced cost of operation of security over the lifetime of a RR SMR.

This section sets out to provide a high-level overview of the application of Secure by Design and its eventual benefits for the secure operation of a RR SMR.

32.5.1.1 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to the SbyD approach.

More detailed CAE is presented in the most recent issue of the following Tier 2 report:

- Rolls-Royce SMR: Secure by Design Methodology [9]
- Rolls-Royce SMR: Secure by Design Report [28]

These Tier 2 documents reference other relevant Tier 3 sources of evidence.

32.5.2 Claims Addressed

The relevant high level (Level 1) Nuclear Security sub-claim is:

[E3S Claim 32.1] Secure by Design: Security risk inherent in the design has been minimised through the application of secure by design principles and a credible secure by design methodology that integrates security considerations into the design process and security measures into SSCs, in a way that is consistent with the operational intent of the RR SMR, and before the application of dedicated security controls.

This Level 1 sub-claim is supported by a set of Level 2 sub-claims, the intention of which is to link them with the various pieces of evidence which. when taken together, demonstrate that the Level 1 sub-claim is met. These Level 2 sub-claims are:

[32.1.1] Relevant analyses of security threat have been undertaken, and in accordance with the Secure by Design concept, where unacceptable risks have been identified design changes have been recommended.

[32.1.2] Potential options for plant layout have been identified and considered to eliminate or reduce associated nuclear security risk.

[32.1.3] The capabilities and likely goals of threat actors are understood.

[32.1.4] A relevant security analysis of the design has been undertaken to identify the ways in which the design may be exploited to cause a radiological release, steal nuclear material or other radioactive material, or compromise sensitive nuclear information.

[32.1.5] Dedicated security measures required to achieve the necessary security Outcome have been proposed.

These sub-claims are tabulated in Appendix A (Section 32.14), which also presents and further decomposition to Level 3.

32.5.3 Features of Secure by Design

The high-level features of the SbyD approach [9] are:

- Security risk shall be evaluated and addressed at source, before considering any existing protection systems or mitigating features of the RR SMR. Efforts should be made to eliminate sources of security risk where this is practical and consistent with the operational purposes of the RR SMR.
- Where it is not possible to eliminate or adequately reduce a source of security risk, features to mitigate it should be integrated directly into the SSC or nuclear process that is the source of the identified risk (where this is practical and consistent with the operational purposes of the RR SMR).
- There shall be identified requirements for security of the RR SMR, and these shall be aligned to the outcomes specified in the SyAPs. These requirements shall be supported by a set of security-related design principles, processes, and practices.
- A structured approach shall be adopted for the engineering of security measures, and security considerations and activities shall be integrated into the programme's systems engineering processes.

A decision-making process that considers both security and safety risks shall be applied to engineering design decisions and concept solution down-selection.

32.5.4 Secure by Design Principles

The Rolls-Royce SMR Limited SbyD Principles, which are presented in sub-section 32.3.3 cover:

- Defence in Depth
- Graded Approach
- Full-life Design and Assurance
- Hierarchy of Security Controls
- Integrated Engineering
- Cross-Domain Risk Management

- Future Proofing Against Emerging Threats.

The allocation of the appropriate SbyD principles to individual SSCs is recorded in the requirements management database [3].

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

32.5.5 Approach to Secure by Design

The Secure by Design Methodology [9] has taken account of Relevant Good Practice and the experience gained to date through interaction with the maturing design.

This approach (which is outlined further in the SbyD methodology [9]) is based around five distinct themes. These themes are:

- Eliminating or reducing security risk at source
- Requirements and principles
- Structured approach
- Engineering integration
- Constraints.

The formalisation of the approach into this methodology allows for its consistent and traceable application. This, in turn, provides a trail of evidence to justify the resultant security solution and support the future secure operation of a RR SMR.

Although currently the application of SbyD is being undertaken with regard to the UK regulatory regime, the intention is that the resultant (generic) security solution should be capable of deployment globally.

The SbyD Methodology [9] was only issued formally in May 2023. The intention for a SbyD approach had existed from the start of concept design prior to the formation of Rolls-Royce SMR Limited in 2021 and entry into the Generic Design Assessment (GDA) in April 2022.

Initially, the security contribution to design was based around providing (informal) advice to design engineers and participation in nuclear safety workshops. The advice provided was based on professional experience, literature reviews and benchmarking exercises within the UK Civil Nuclear industry.

During this period emphasis was placed on understanding the requirements for protection from sabotage (including vital area assessment and identification) and providing advice on the security measures which would make up a Physical Protection System (PPS) or required as part of a Cyber Protection System (CPS). From a security point of view, the documents and learning from this phase have been incorporated into later documents or simply superseded.

The application of SbyD was based around a Secure by Design Guidance document [29] which was produced by Rolls-Royce Civil Nuclear as part of a Department of Business, Energy and Industrial Strategy (BEIS) research contract. The research undertaken included a consultation exercise across

the UK Civil Nuclear Industry. This (BEIS) guidance was an input into the development of the Rolls-Royce SMR SbyD methodology.

32.5.6 Small Modular Design

A key criterion for the RR SMR is a compact design. SbyD can help to realise this vision by reducing security risk at source, thereby reducing the reliance on dedicated security measures that would occupy additional space in the RR SMR.

This design, together with its modular structure present a different security environment to that presented by traditional larger nuclear power plants. For example, a relatively compact footprint challenges the traditional approaches to nuclear security, which partially rely on large structures and open ground to delay and respond to adversaries.

Conversely, there are also potential benefits to security. For example, the compact nature means there is less area to cover by detection systems and highly protected areas are likely to be concentrated in smaller areas.

Based on security involvement to date with the maturing design and the professional experience of Security Subject Matter Experts (SMEs), a summary of the main identified security benefits and vulnerabilities associated with 'novel' design features is presented in Table 32.5-1.

Table 32.5-1: Potential Security Aspects of a Compact and Modular Design

Design Feature	**Potential Security Benefits**	**Potential Security Hazard**
Berm	Hostile vehicle mitigation (HVM), camouflage	Attacker/Defence interface
Hazard Shield	NM all contained inside this feature making control easier.	Easier for threat actor to sabotage multiple SSCs if they gain access.
Modularisation	Allows for multiple security layers. Potential sacrificial systems	Easier impact across multiple systems. Common design across the fleet
Shape	Greater visual coverage & more easily defensible.	Distinctive
Compact	Travel distance. Smaller staff numbers reduce insider threat.	Easier impact across multiple systems
Shell Roof	Mortar defence. Reduces external visibility	TBC

Whilst this preliminary identification of potential benefits and vulnerabilities has (informally) informed the preliminary application of SbyD, it is recognised that their identification is based around (as yet) unjustified assumptions.

These assumptions are tested as the security analyses (see sub-section 32.5.10) are undertaken on the maturing design and in the subsequent development of the ISS for the RR SMR.

32.5.7 Overview of the Secure by Design Methodology

The SbyD methodology is spread across three stages (see Figure 32.5-1). These stages and steps are:

- Stage 1: Identification of work packages relevant to SbyD –
    - Step 1, Initial Assessment
    - Step 2, Security Led Assessment
- Stage 2: Security support to the work package during preliminary concept design and selection to eliminate or reduce sources of security risk
- Stage 3: Integrating security measures –
    - Step 1, Establishing and applying the Environment, Safety, Security and Safeguards (E3S) Principles to the design
    - Step 2, Identifying potential security vulnerabilities through:
    - Step 3, Defining Initiating Events of Malicious Origin (IEMOs)
    - Step 4, Defining Security Defence in Depth (ISS concept design)
    - Step 5, Defining Security Requirements
    - Step 6, Categorisation and classification.

The initial assessment, by the system owner, provides early security-informed input into the design process by building upon a number of assumptions and judgements prior to a formal application of the methodology. This supports early application of the SbyD principle at a time where the ability to influence the design is arguably at its greatest.

Any assumptions made prior to the formal application of the methodology, should be recorded within a design record (e.g. DR0) and a justification provided.

Rolls-Royce SMR Limited has produced a 'Threat Interpretation' document [8]. This document collates threat intelligence from several sources which is interpreted in the context of the RR SMR to present a single coherent statement of adversary capability.

The 'Threat Interpretation' is used to support security analysis activities. It is also used to support design decisions in relation to SbyD, the validation of security features and verification of security requirements.

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

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

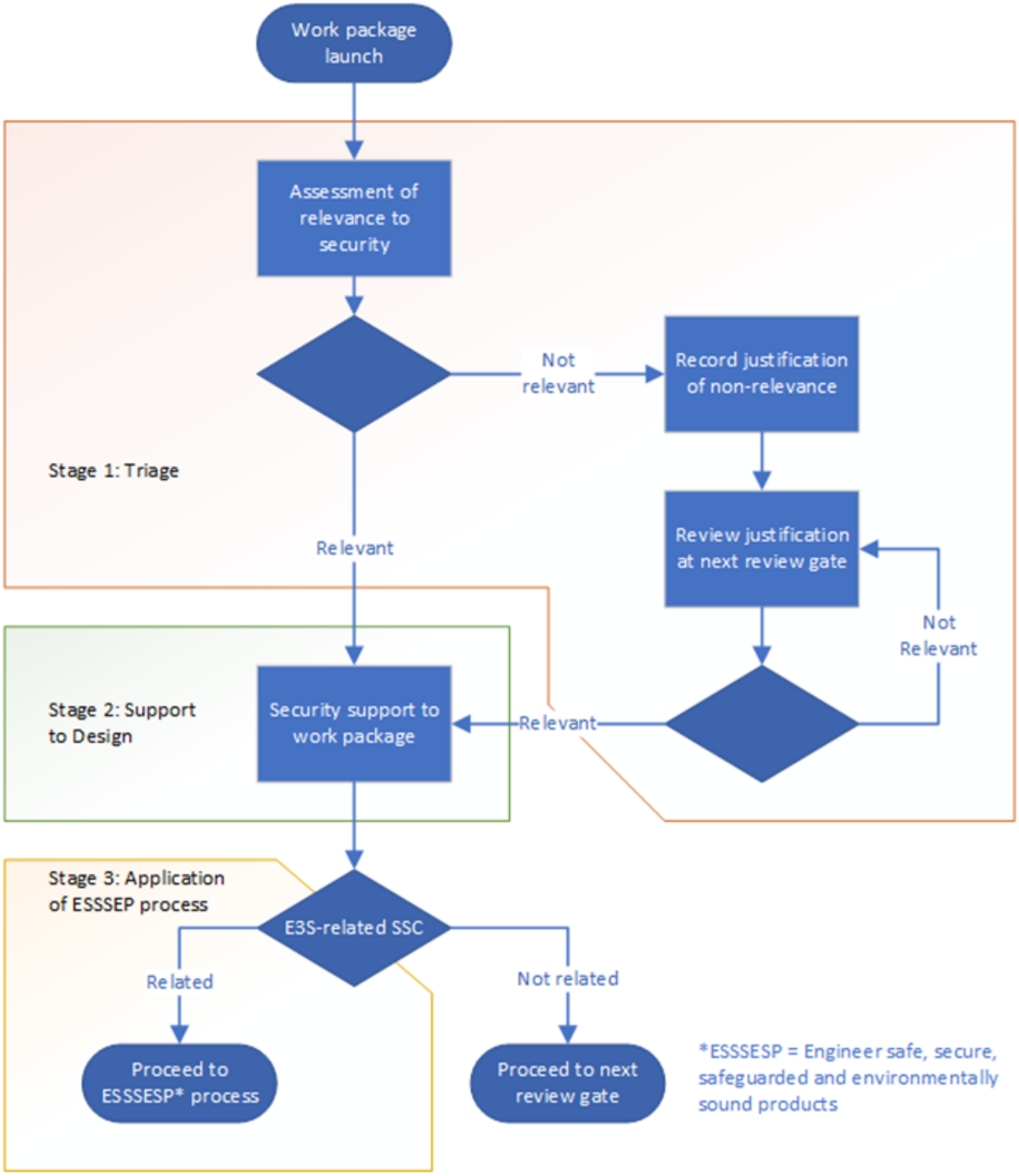


Figure 32.5-1: Secure by Design Methodology Overview

32.5.8 Security Categorisation and Classification

The purpose of the Functional Security Categorisation and Classification Methodology [24] is to describe the principles and methods for:

- Identifying security functions

- Categorising security functions according to their importance
- Identifying the SSCs delivering security functions
- Classifying the SSCs according to their contribution in delivering the identified security functions.

32.5.8.1 Safety Categorisation and Classification, and Cyber Security Degrees

The security functional categorisation and classification is a separate scheme to the nuclear safety functional categorisation and classification scheme [30]. This allows for fundamental differences in how security and safety consider the frequency of potential initiating events and IEMOs. The overall approach is consistent.

Cyber security degrees are an independent but related concept restricted to C&I and information systems, where they are assigned to systems, or parts of systems, to facilitate secure architectural design and the application of the Cyber Security Risk Assessment (CSRA) methodology [31].

The application of security degrees is informed by the safety or security consequences arising as a result of a successful cyber-attack against the C&I system under consideration. This usually takes note of existing safety or security categorisation and classification. Some systems may have significant consequences associated with them outside of safety or security (for example financial, economic, privacy and safeguards) and thereby have a Security Degree applied to them independent of safety or security classification.

32.5.8.2 Security Functions

Physical Security Functions

The physical security functions mirror those defined in the ONR SyAPs [7] and Annexes [16] and are aligned to the key functions of a physical protection system defined in international relevant good practice [10].

These physical security functions are: Deter, Detect, Delay, Assess, Control of Access, and Minimise Insider Threat.

Cyber Security Functions

The cyber security functions are aligned with the categories of activities outlined in the ONR SyAPs [3] and the National Institute for Standards and Technology (NIST) framework for improving critical infrastructure cyber security [27]

These physical security functions are: Identify, Protect, Detect, Respond and Recover.

32.5.8.3 Methodology to Categorise Security Functions

Categorisation Principles

The categorisation of security functions supports a graded approach to the design of protection systems. Sufficient categories should be defined to support this goal. The assignment of categories to security functions should be proportionate to the consequences associated with the failure of

those functions and the threat. The categorisation scheme is aligned to the Outcome and Posture tables in the classified annexes to SyAPs [16].

Security Function Categories

Security functional categories are assigned to functions using Posture as a metric for consequence. The category applied to a security function reflects the consequences of the failure of the security function:

- Category A is assigned to functions that play a principal role in achieving the desired security Outcome, where failure would directly lead to the most severe consequences. Functions assigned this category are expected to provide continuous or immediate protection by directly interrupting an attack scenario, and to maintain their effectiveness when exposed to threat capabilities.

- Category B is assigned to functions that play a complementary role to Category A functions in achieving the desired security Outcome, by providing defence in depth where this is required in either Annex C (for physical security) or Annex H (for cyber security) in the SyAPs classified annexes [16]. Category B may also be assigned to functions that play a principal role where their failure would lead to less severe consequences, for example where protecting a lower category of VA or NM/ORM, or where other independent measures are in place to prevent or mitigate the consequences.

- Category C is assigned to functions that play a complementary role to Category B functions in achieving the desired security Outcome, i.e. by providing defence in depth where this is required in either Annex C (for physical security) or Annex H (for cyber security) in the SyAPs classified annexes [16]. Category C may also be assigned to functions that play a principal role in achieving a baseline level of security in accordance with the desired security Outcome.

32.5.8.4 Methodology to Classify SSCs Delivering Security Functions

Classification Principles

The classification of SSCs delivering security functions supports a graded approach to their design, implementation, integration, commissioning, maintenance and operation. A single SSC may deliver multiple security functions subject to the diversity and independence requirements.

Security SSC Classifications

SSCs that deliver security functions can be either dedicated security SSCs (i.e. sub-systems and components of the PPS and CPS) or non-security SSCs that, by their nature, have the capacity to deliver security functions (for example elements of the building structure).

Three classes are defined for the SSCs delivering security functions: Class 1, which has the most stringent requirements, Class 2, and Class 3, which has the least stringent. The classes are assigned to SSCs delivering security functions according to the most significant security function that they deliver.

The SSCs are classified according to the most significant security function allocated to it. For components, the contribution of the component in delivering the function shall also be considered

when classifying the component, as not all components of the SSC are critical in delivering the function.

Analysis of the effects of failure of the component on the ability of the SSC to deliver the security function are also be considered, for example through a Failure Modes and Effects Analysis (FMEA). Where failure would lead to loss of the function, the component shall be classified as though it was the sole or principal means.

32.5.9 Interaction with Engineering Design

As noted above, the interaction of Security SMEs with the maturing engineering design has developed over time, leading to the development and formal issue of the SbyD Methodology [9].

This methodology comprises three stages as follows:

- Stage 1 – Identification of Work Packages Relevant to SbyD
- Stage 2 – Support to Design
- Stage 3 – Integrating Security Measures

Within the Rolls-Royce SMR Limited Integrated Management System (IMS), the primary process which should ensure the integration SbyD into engineering design (and the identification of Security SMEs as stakeholders) is IMS Process C3.2.2.3, Application of the 'Engineer safe, secure, safeguarded and environmentally sound products' [32].

A SbyD-Database is being used to track the interactions between SbyD and engineering. This database tracks progress through Stage 1 to Stage 3 and contains references to evidence of this progress. This database continues to be developed and refined both as a primary management tool and (potentially) a summary of technical information.

Further detail of this interaction is provided in the Secure by Design Report [28].

32.5.10 Security Analyses

Stage 2 of the SbyD Methodology is supported through detailed security analyses. These analyses, which seek to address the four main regulatory themes for protection of the RR SMR are:

- Categorisation for Theft Methodology [33]
- Cyber Security Risk Assessment [31] and review of CBSy [34]
- Vital Area Identification and Categorisation Methodology [35]
- Protection of Sensitive Nuclear Information [36].

There are linkages between that could lead to sharing information (for example regarding the NM and ORM inventory) between the analyses streams. Further, one analysis could throw to another (for example if a SSC identified during VAI&C has an associated digital control, then CSRA would be required, or vice versa, if CSRA identified a vulnerability in C&I associated with a safety system this would indicate that VAI&C should also be considered).

For example, if a system contains or handles NM it requires analysis from a point of view of theft and sabotage; if the system involves digital C&I, the CSRA is also relevant. Further, the requirement for any associated CSRA should form part of all VAI&C analyses.

The assessment of systems or analysis about the protection of SNI, or the assurance of CBSy, is not covered within this iteration of the SbyD report and its inclusion in the above list of analysis types was for completeness only.

These are not one-off analyses but are repeated against the maturing design to assess any reduction in vulnerability resulting from the inclusion of security requirements in design (typically as part of the development of the ISS).

Post DR3, if any changes are proposed to an SSC design, the Manage change IMS Process [37] requires Security SMEs to be informed of such and an assessment made of any implications of the change on security. This might involve repeating the relevant security analyses.

32.5.11 Integrated Security Solution

After the issue of the ONR SyAPs [7], the regulatory regime for nuclear security in the UK has become more permissive. Dutyholders are now required to meet certain Security Outcomes and Postures [16]. These outcomes are determined from the results of security analyses undertaken to assess risk of sabotage, theft (of NM and/ORM) and cyber-attack.

Historically, analysis was undertaken on a final (or near complete) engineering design for a facility. The resultant security solutions typically comprised a PPS and a CPS which were “add-ons” to the engineering design of, not part of it. The PPS and CPS were integrated to the extent that there was physical protection of cyber systems.

With increasing use of digital control systems and an ever more sophisticated cyber threat, the requirements for CPS have grown, including the necessity to protect the CPS both virtually and physically. This, together with an increasing threat from blended attacks (combined physical and cyber-attacks), has driven the increasing integration of the PPS and CPS.

The SbyD approach drives the combination of the PPS and CPS into an ISS for the RR SMR which comprises a combination of:

- The security benefit within engineering design
- Design features which provide a security benefit
- Identified design modifications which to seek to address security vulnerabilities and (ideally) remove or reduce such
- Dedicated security SSCs, that is SSCs whose primary purpose is address residual risk through the provision of security functions such as deter (for example, fences and other barriers), detect and assess (for example, CCTV, alarms etc.), and delay (for example, security doors).

The framework for the development of the ISS is outlined in Section 32.9). Subsequent issues will document the development of the ISS in conjunction with the maturing engineering design of the RR SMR.

The iterative development of the ISS seeks to identify any further design modifications that can contribute to achieving the required outcomes. The iterative process is undertaken until no further possible design modification are identified/possible. At this stage, the output from this system engineering process are the requirements for the integrated PPS and CPS to address the residual risk.

This ISS provides the basis for the subsequent development a Nuclear Site Security Plan (NSSP) (in UK) or similar (worldwide) (see Section 32.11). When completed, the ISS should provide a future Operator/Dutyholder with:

- An understanding of the whole of the security solution for the RR SMR, how it has been developed, and the assumptions inherent in its design and development.
- An understanding of how the ISS for the RR SMR should be operated (Tech Specs) and the assumptions inherent in its operation.
- The Operator owned risks that need addressing as part of its implementation

Techniques such as Vulnerability Assessment, of the physical or cyber protection system, can help identify if there are any remaining gaps in the security solution that could be exploited by an adversary, and assist in demonstrating that the applicable Security Outcomes have been achieved.

32.5.12 Constraints and Deconfliction

During the design phase of the RR SMR, a number of requirements are taken into account in the design. These requirements are derived from a variety of sources to drive and influence the design. Capture and management of these requirements is described in the Define and Manage Requirements process, C3.1.1 [38].

At various stages of design development reviews are conducted to ensure alignment of the design with the E3S Design Principles [23] and Requirements [39] as part of the design process.

Security measures do not exist in isolation and can impact the other key performance criteria of the RR SMR; therefore, any proposed measures, intrinsic or extrinsic, must be:

- Consistent with operational purposes of the RR SMR
- Compatible with operations, safety (assumed to be both nuclear and conventional) and nuclear safeguards.

Nuclear Safety is at the heart of the ONR's Unifying Purpose Statement with the SyAPs [7] that is, the overarching objective a nuclear security case is to "protect the public from the risks arising from a radiological event caused by the theft or sabotage of NM/ORM and supporting systems or through the compromise of SNI".

It is clear, therefore, that security measures are included within a design to enhance the safety of the system and to ensure safety functions are delivered as intended by the design.

The Definition Review process [40] states that it must be demonstrated, to the relevant experts on the review, that the requirements specified have been achieved. Where there is dispute or disagreement, additional technical reviews may be conducted, including all relevant experts, to resolve the dispute.

If for any reason a technical review cannot resolve the dispute, it will be referred to next level of managerial, engineering or technical control within Rolls-Royce SMR Limited, as allowed for within the E3S Requirements and Analysis Arrangements [39].

32.5.13 Outputs from Secure by Design

The Secure by Design methodology is more the formalisation of a philosophy or an approach rather than methodology with a defined output. The primary function is to link the security analyses to the development often ISS and link the development of the security case with engineering design.

At a high-level, the outputs from SbyD (in conjunction with the development of the ISS) can be summarised as:

- Influence (informal) and requirements (formal) on the engineering SSCs to reduce security risk and vulnerabilities
- High-level requirements for the design of PPS and CPS measures to address residual security risk.

Future issues of this Chapter 32 will provide a summary of these high-level output (with reference to relevant Tier 2 and Tier 3 sources).

Information (in the form of metrics) will also be provided to illustrate the progress with the application of SbyD across engineering design (as tracked in the SbyD Database).

32.5.14 Future Work

Application of the SbyD methodology is in on-going activity. To date, interactions with engineering design has focussed around Stage 1. Following the pilot studies for the security analyses, and in conjunction with SSC designs approaching DR3, these interactions are moving into Stage 3. This is discussed further in the sections discussing CfT (Section 32.6), CSRA (Section 32.7) and VAI&C (Section 32.8).

Improvements have been identified for the SbyD Methodology [9] since the release of Issue 2. These improvements relate mainly to requirement for clarity and strengthening of the links that SbyD makes between the security analyses and the development of the ISS. These improvements will be incorporated into a future issue of the SbyD methodology.

32.6 Categorisation for Theft

32.6.1 Introduction

It is a regulatory requirement that the GSR identifies appropriate security measures to protect Nuclear Material and Other Radioactive Material (NM/ORM) from theft. The categorisation of the material is linked to the Security Outcomes, Postures and Responses (SOPRs) in SyAPs [16] used to determine the levels of security that should be applied to protect the material.

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

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

Rolls-Royce SMR Limited have developed a CfT Methodology [33]; an overview of which is presented in this section.

CfT should be based on the full inventory for the site or facilities. As yet, a definitive inventory cannot be established for the RR SMR. To demonstrate the methodology, a Pilot Study [41] was undertaken.

32.6.2 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to CfT. More detailed CAE is presented in the most recent issue of the following Tier 2 reports:

- Rolls-Royce SMR: Categorisation for Theft Methodology [33]
- Rolls-Royce SMR: Theft of Material and Categorisation Report [42].

This Tier 2 document references other relevant Tier 3 sources of evidence.

32.6.3 Claims Addressed

The relevant high level (Level 1) Nuclear Security sub-claim is:

[E3S Claim 32.3] Protection from Theft: Material at risk of theft has been identified through the application of a Categorisation for Theft Methodology. Security measures have been identified, and applied in a Graded Approach, to minimise the risk of theft. These security measures form part of an Integrated Security Solution (ISS) for the generic RR SMR.

This Level 1 sub-claim is supported by a set of Level 2 sub-claims, the intention of which is to link them with the various pieces of evidence which, when taken together, demonstrate that the Level 1 sub-claim is met. These Level 2 sub-claims are:

[32.3.1] The Nuclear Material (NM) & Other Radioactive Material (ORM) inventories have been categorised, using an appropriate Categorisation for Theft agreed methodology, for the purpose of identifying the level of protection from theft that is required.

[32.3.2] Following the Categorisation for Theft of the Nuclear Material (NM) & Other Radioactive Material (ORM) inventories, any applicable recommendations for risk reduction were proposed and reported to the relevant design team.

[32.3.3] The security requirements identified through Categorisation for Theft Methodology were developed further as part of an overall Integrated Security Solution for the generic RR SMR, which addresses physical, cyber and blended threats.

These sub-claims are tabulated in Appendix B (Section 32.15) which also presents and further decomposition to Level 3.

32.6.4 Overview of Categorisation for Theft Methodology

A CfT Methodology [33] has been developed for use by Rolls-Royce SMR Limited in the development of the ISS for the RR SMR. Although this methodology has been developed for application the UK, it is based on IAEA guidance and can readily be adapted for application under other regulatory regimes.

The methodology is consistent with RGP including:

- Office for Nuclear Regulation (ONR) Security Assessment Principles (SyAPs) for the Civil Nuclear Industry 2022 Edition, Version 1 [7]
- ONR Nuclear Security Technical Assessment Guide, Categorisation for Theft (CNS-TAST-GD-6.1) [17].

The starting point for this security analysis is an inventory of NM, ORM and radioactive sources that will be present (or is expected to be) on a RR SMR throughout its operational lifecycle. Categorisation of these materials is undertaken against the relevant table in the Annexes to the ONR SyAPs [16].

Currently, the available design information does not allow for full inventory for the generic RR SMR to be identified. To trial the method, a pilot study was undertaken.

As the design matures, and a full inventory is available, a formal full categorisation will be carried out using the methodology outlined in this Section. This will include for a (whole) site categorisation and a categorisation for individual buildings holding NM, ORM or radiological sources.

32.6.4.1 Categorisation of Nuclear Materials

Categorisation of NM for theft is undertaken in line with Table 1 in SyAPs Annexes [16] which provides four categories for NM (Categories I, II, III and IV). This is based on the potential attractiveness of the NM from a proliferation perspective and does not apply when considering malicious acts other than constructing a Nuclear Explosive Device (NED).

Figure 32.6-1 summarises the steps in the categorisation of NM. Further details are provided in the methodology [33].

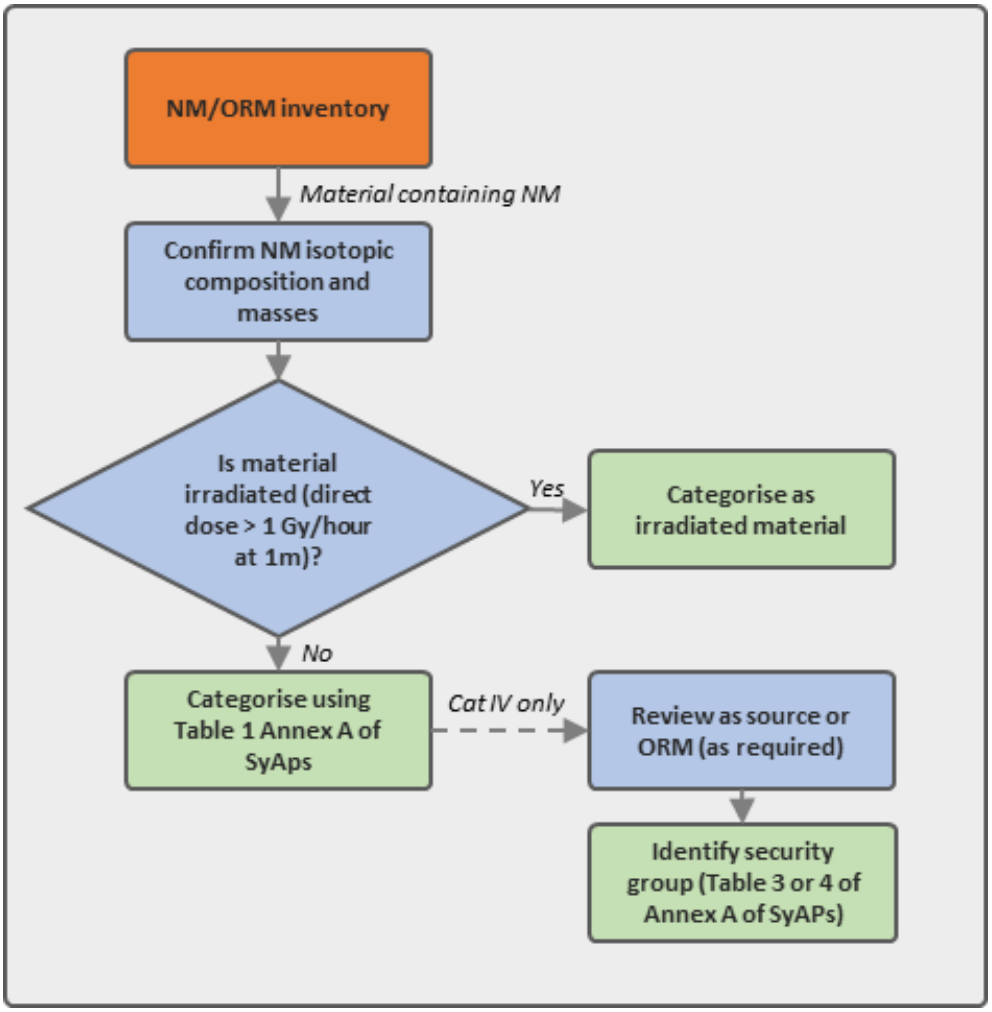


Figure 32.6-1: Categorisation of Nuclear Materials (NM)

NM is fissile material as defined in The Energy Act 2004 (as amended) [43]. The categorisation of the NM simply reflects the total amount held on the site and does not reflect the ease by which the NM could be stolen nor the means by which such material could be processed or refined to separate fissile material from other materials with which it may be mixed. The physical characteristics of the NM can, however, be taken into account through proportionate protective measures.

32.6.4.2 Categorisation of Radioactive Sources

A radioactive source may be defined as a relatively small package of radioactive material to be used for a defined purpose, typically detector calibration by health physics, inspection purposes or to provide a neutron source for reactor start-up. Usually, such a source would be stored within a shielded container when not in use.

This categorisation scheme places radioactive sources into one of four security groups which relate to five categories. Radioactive sources in Category 1 are the most harmful because they can pose a very high risk to human health if not managed safely and securely, such as strong medical sources. Many of the examples of sources within Table 3 of the SyAPs Annexes [16] relate to medical or

industrial applications and a direct read-across to radioactive sources at the RR SMR site may not be straightforward in all cases.

32.6.4.3 Categorisation of Other Radioactive Materials

ORM on the RR SMR site could include intermediate-level waste (ILW) and low-level waste (LLW), for example used filters and ion exchange columns. The inventory of ORM should also consider the potential variation of this inventory during the RR SMR lifecycle which should also be considered within the categorisation process.

Figure 32.6-2 summarises the step in the categorisation of NM. Further details are provided in the methodology [3].

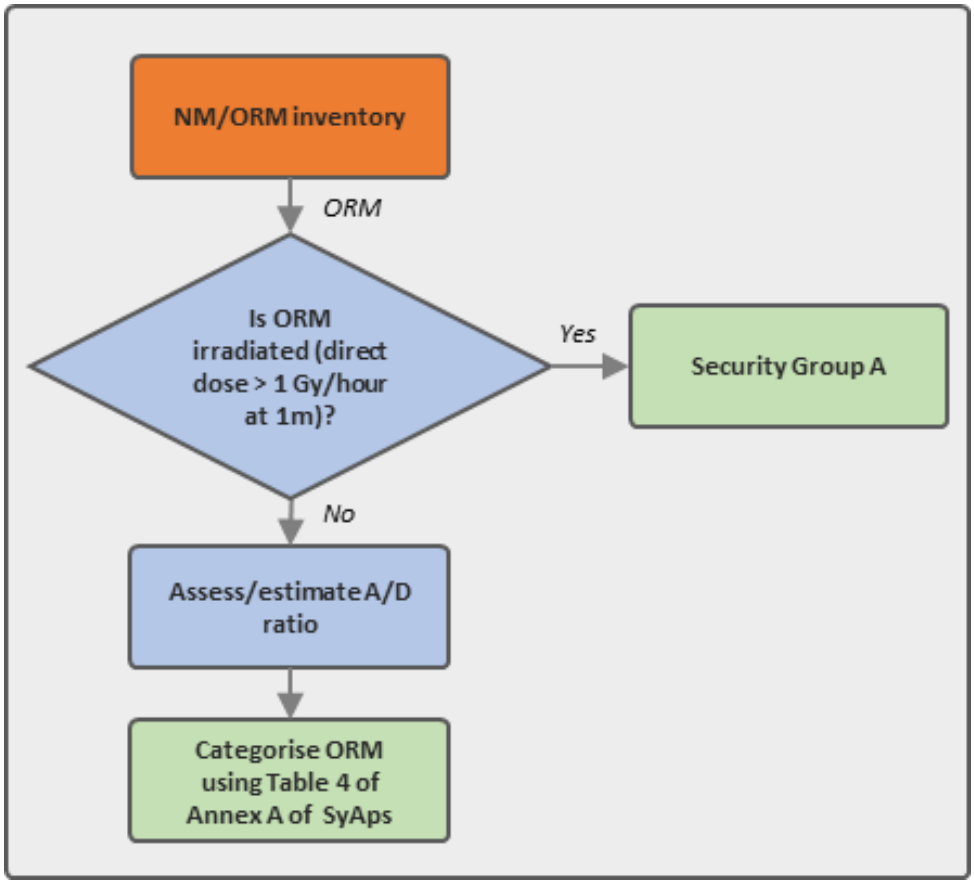


Figure 32.6-2: Categorisation of Other Radioactive Material (ORM)

Categorisation of ORM is based on Table 4 the SyAPs Annexes [16]. ORM with a radiation output exceeding the threshold dose is categorised as Security Group A to D [16].

The categorisation of the ORM simply reflects the total amount held on the site and does not reflect the ease by which the ORM could be stolen nor the means by which such material could be processed or refined to separate fissile material from other materials with which it may be mixed. The physical and chemical characteristics of the ORM can be taken into account through proportionate protective measures.

32.6.4.4 Identification of Areas Requiring Protection from Theft

In conjunction with the categorisation of NM and ORM against theft, it is necessary to also identify those areas of the plant which require protection from theft. Locations requiring protection from theft are identified in plot plans. The plot plans also show the most onerous categorisation of the NM, sources and ORM Security Groups associated with the NM, ORM and/or sources within the identified areas.

Where an area of the plant requires protection from both theft and sabotage, the requirements should be reviewed to ensure that any potential conflicts are resolved and that both sabotage and theft-related attacks are addressed by the security solution. The SbyD principle should be applied when considering potential vulnerabilities and potential design changes to improve robustness against theft due to design or operational changes [9]. This process is summarised in Figure 32.6-3.

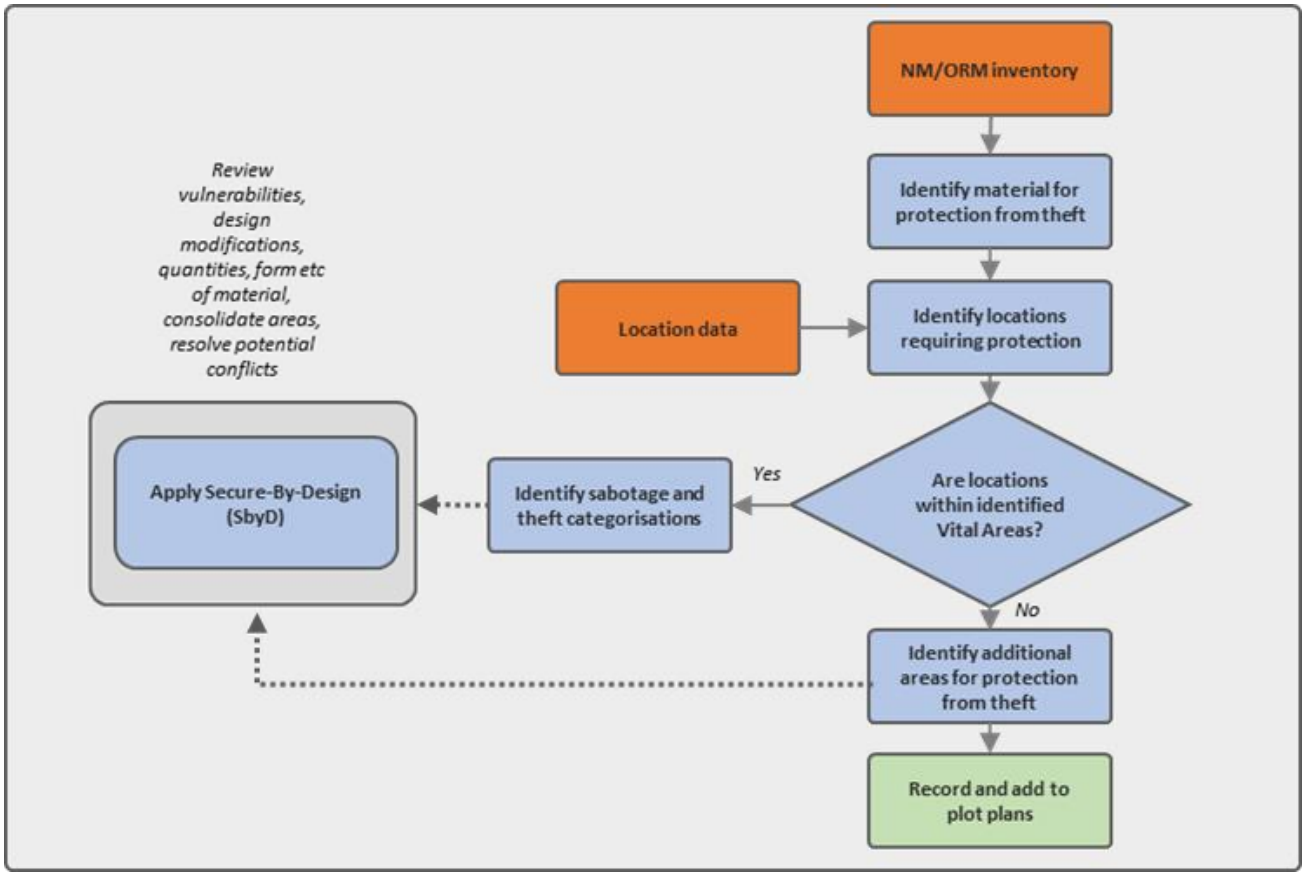


Figure 32.6-3: Identification of Theft Protection Areas

32.6.4.5 Review of Categorisation for Theft

During the lifecycle of the RR SMR, it is likely that the activity, locations and quantities of NM, ORM and sources vary as waste is accumulated, fuel is used and operational requirements or the design changes. Hence, it is important that the categorisation for theft and locations requiring protection from theft are regularly reviewed to ensure that they remain appropriate for the site or individual facility.

Review of the identified categorisation for theft and theft protection locations process may be triggered from events, including:

- Planned changes to inventory, activity, form, volume of NM, ORM or sources

- Reduction in direct dose rate from NM or ORM previously identified as 'irradiated material'
- Accumulation of material
- Changes to storage locations
- Amendments to Categorisation requirements (for example, SyAps Annex A)
- Changes to Vital Areas (for example, where sabotage protection requirements are no longer bounding or conflicts arise)
- Unplanned changes.

In the event of a significant change, the appropriate aspects of the theft categorisation methodology are repeated to confirm, or revise, the identified categorisation. In such cases, the SbyD methodology [9] should also be applied to ensure that robustness against theft of material is designed-in where appropriate.

32.6.5 Outputs from Categorisation for Theft

In future issues, this section will summarise the outputs from CfT methodology; and give an overall categorisation for the generic RR SMR. This summary will reference the Tier 2 Report [42] and other relevant Tier 3 evidence.

Information regarding the full inventory of the RR SMR across the operational lifecycle is not yet available. The text below is based around the output from the pilot study only.

32.6.5.1 Inventory of NM/ORM for RR SMR

In future issues of this Chapter, this sub-section will summarise the inventory of NM/OR through the operational life of the RR SMR.

32.6.5.2 Secure by Design Analysis

In alignment with the SbyD approach to, this theft categorisation methodology is used to identify whether a design or process modification can be made which can eliminate the need to provide protection against theft to a particular area (for example removal of NM, ORM or sources) or reduce the categorisation of the material within a particular area (for example by reducing the amount or changing the composition of material within an area).

32.6.5.3 Categorisation of Material for Theft

To demonstrate the application of the methodology, a pilot study was undertaken based around the inventory associated with Fuelling Block [7]. This identified the presence of new fuel, spent fuel and partially spent fuel within the pilot study area.

Based on a data for typical PWR fuel, an indicative categorisation for the spent fuel is Category III [41] New fuel, which is treated as 'unirradiated' material (by virtue of its low direct dose) [16] has an indicative categorisation of Category III.

In future issues of this Chapter, this sub-section will set out the categorisation (for theft) for the RR SMR, based on a full inventory for the design. This will include a categorisation at both site level and for individual buildings.

32.6.5.4 Locations where NM/ORM will Require Security Protection from Theft

To demonstrate the application of the methodology, a pilot study was undertaken based around the inventory associated with Fuelling Block [7]. Example plot plans were prepared based on the findings of this pilot study [7].

In future issues of this Chapter, this sub-section will set out the locations (across the RR SMR) where NM/ORM will require security measure to be put in place as protection from theft.

32.6.5.5 Minimisation of Areas to be Protected

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

A key aspect will be the interface with the identification of Vital Areas (see Section 32.6.4.4). In this case, areas of the plant may require protection from both sabotage and theft and application of the SbyD can be used to provide an optimised security solution for both requirements.

32.6.6 Integrated Security Solution

The output from the CfT is taken forward into the development of a PPS as part of the overall ISS. This is undertaken as part of the overall SbyD Approach.

The protection afforded to the identified NM/ORM (and the areas where they are located) is graded depending on the sabotage-related dose or the NM, ORM or sources located within them, as follows (based on Annex C of the SyAPs Annexes [16].

- The PPS outcome for areas containing NM, ORM and/or sources that are also identified as VAs is bounded by the PPS outcome for sabotage.
- The PPS outcome for areas containing NM, ORM and/or sources that are also identified as VA depends on the higher of the two PPS outcomes for sabotage or theft.
- For areas for areas containing NM, ORM and/or sources which are identified as baseline areas against sabotage, the theft categorisation applies.

32.6.7 Future Work

The CfT methodology trial has achieved its aim of identifying and categorising NM/ORM in the sample area chosen for the pilot study and demonstrating the pragmatic applicability of the process.

The process will be formally applied to the rest of the RR SMR design when a more definitive inventory has been established.

All analysis aligns closely with VAI&C in support of delivering SbyD, and in turn informs the design of a PPS as part of the ISS.

The application of the CfT methodology is not intended to be a one-off but rather an iterative process. For example, it would be repeated (post DR3) if there were to be any significant changes in design [11].

32.7 Cyber Security

32.7.1 Introduction

The Security Case for the RR SMR demonstrates how the Cyber Protection System (CPS) requirements are met to provide protection of nuclear technology and operations. This applies to:

- Control and Instrumentation (C&I) systems with a focus on Computer Based Systems Important to (Nuclear) Safety (CBSIS)
- Computer-Based Security systems (CBSy)
- Computer Based Systems Essential to Safe Operations (CBSESO).

These systems should be protected against a cyber-attack which could result in:

- The release of radiation which could cause harm to RR SMR staff, the general public or the environment
- Theft or unintended release of radioactive materials outside the site boundary
- Corruption or Compromise of SNI
- Impacts on the availability of systems that are essential to safe generation of electricity or transfer onto the grid
- impacts on the availability of nuclear safety systems.

When assessing potential radiological release, the consequences of the cyber-attack would be those within the safety case. A standalone cyber attack should not result in a greater consequence (higher dose or release) than that used to allocate safety class. A blended attack (cyber and physical) could result in a significantly increased consequence, for example by linked sabotage of physical containment allowing off-site dose.

Rolls-Royce SMR Limited has developed a CSRA Methodology [31], an overview of which is presented in this section. This methodology has been demonstrated through a pilot study [44] prior to application across the RR SMR.

This Section summarises Issue 2 of the CSRA. Requirements for improvement and clarification are recognised, and the methodology is currently under review.

32.7.2 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to the topic are of Cyber Security. More detailed CAE is presented in the most recent issue of the following Tier 2 report:

- Rolls-Royce SMR: Cyber Security Risk Assessment Methodology [31]
- Rolls-Royce SMR: Cyber Security Report [45].

These Tier 2 documents reference Tier 3 sources of evidence, including that relating to the application of the methodology.

32.7.3 Claims Addressed

The relevant high level (Level 1) Nuclear Security sub-claim is:

[NSy 3.0] Cyber Security & Information Assurance (CS&IA): The risks to all digital assets (including Operational Technology [OT] and Information Technology [IT]) associated with the generic RR SMR shall be reduced to an acceptable level through the use of CS&IA as part of a larger Cyber Protection System (CPS), within an Integrated Security Solution (ISS). Risks to be mitigated include sabotage resulting in an Unacceptable radiological Consequence, the theft of nuclear/radiological materials, the compromise of sensitive nuclear information, as well as lesser consequences such as plant interruptions, industrial hazards and lesser radiological consequences.

This Level 1 sub-claim is supported by into a set of Level 2 sub-claims, the intention of which is to link them with the various pieces of evidence which, when taken together, demonstrate that the Level 1 sub-claim is met. These Level 2 sub-claims are:

[32.3.1] – Policies and procedures shall be put in place to manage cyber risk in accordance with recognised international standards and RGP, with defined roles and responsibilities, and communication routes.

[32.3.2] – Cyber security risks shall be assessed using threat-based risk assessment process utilising the RR SMR Threat Interpretation to provide a graded security approach based on the system consequences.

[32.3.3] – Cyber security control sets shall be implemented to reduce cyber security risks to an acceptable level, in a graded approach based on the consequences of system compromise and the skill of the threat actor.

[32.3.4] – Sensitive Nuclear Information shall be subject to appropriate security controls to maintain its confidentiality, integrity and availability.

[32.3.5} – Cyber security controls shall be implemented was part of an Integrated Security Solution (ISS) in conjunction with physical Regulatory Framework for the Nuclear Security Case

These sub-claims are tabulated in Appendix C (Section 32.16), which also presents and further decomposition to Level 3.

32.7.4 Overview of Cyber Security Risk Assessment Methodology

A Cyber Security Risk Assessment Methodology (CSRAM) [31] has been adopted to identify and manage cyber risk through the life cycle of the design and operational plant of the RR SMR. This methodology is based on relevant international standards that are either nuclear focused or have been modified to fit the expectations within the Civil Nuclear Industry.

The CSRAM is a seven-step process which is repeatable over the life cycle of the RR SMR. The cyber security risk assessment methodology for single CBSIS or CBSy systems is presented within Figure 32.7-1.

The objectives of the CSRAM are:

- Risk Identification: This identifies cyber risk through a consistent and repeatable process. This is based on the most mature industrial cyber security risk assessment standard currently available, BS EN IEC 62443-3-2 [46] and adapted for use within Civil Nuclear Sector.

- Risk Scoring: Where cyber risks are identified, the methodology permits for risk scoring. Risk scoring is informed through the Threat Interpretation and consequence analysis rather than probability. Threat Interpretation shall include intent and sophistication of threat actors, informed through the UK Design Basis Threat (DBT), national and international threat intelligence sources.

- Risk Treatment: Those risk scores are then moved through a consistent risk treatment process to achieve the desired outcomes from ONR SyAPs [16]. Identified control sets are included within the secure by design process.

- Risk Management: Manages and documents the ownership of risk through the life cycle of the plant whether that is from designers, through to future operators.

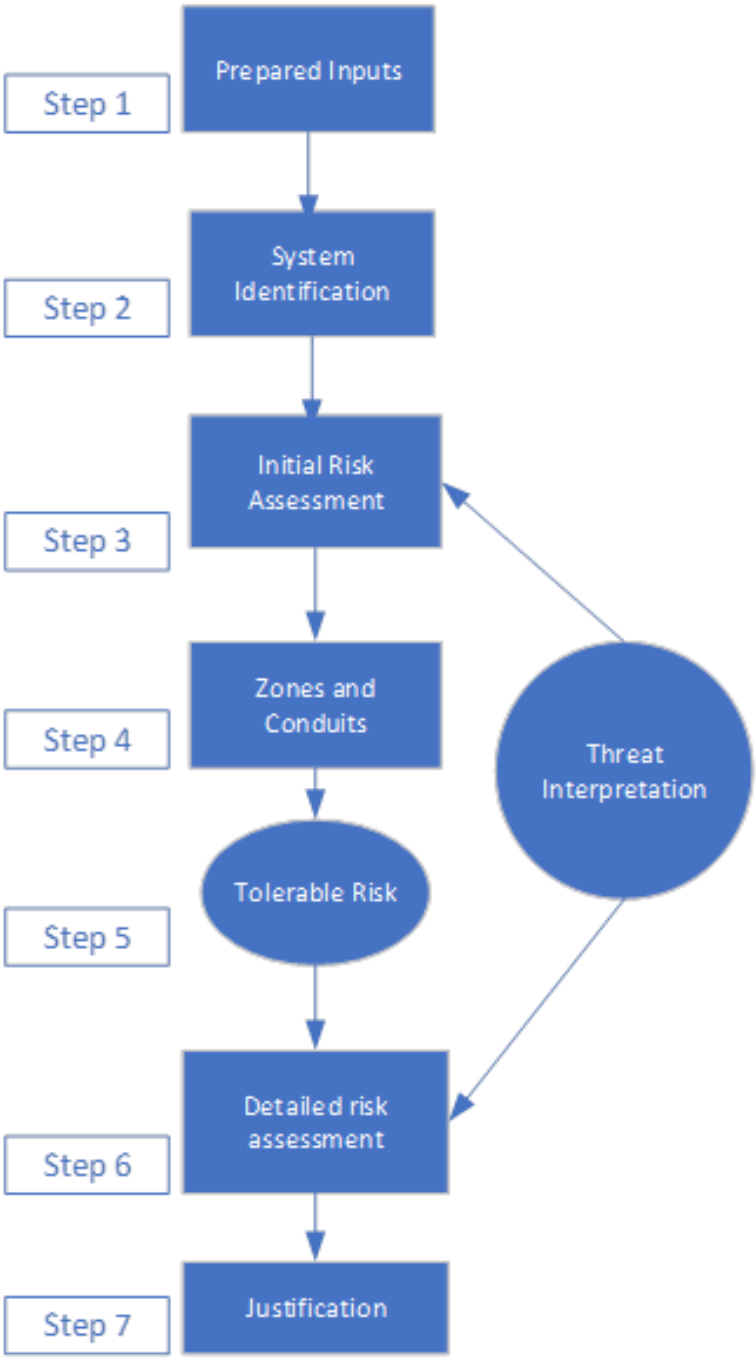


Figure 32.7-1: Overview of Cyber Security Risk Assessment Methodology

32.7.4.1 Step 1 – Prepared Inputs

CBSIS systems are identified within the RR SMR design as detailed within the safety case documents (Stage 1 of SbyD [9]). The interaction between these CBSIS and SSCs claimed within the fault schedule are identified in discussions with the C&I Design Team. CBSy systems will be identified from the ISS.

Technical information is gathered for each CBSIS and CBSy to determine its functionality, the technology upon which is it based and interconnections both within the system and to other CBSIS or supporting systems. Dependencies to supporting systems is also be identified. This information is obtained from the current safety case and the C&I design documentation.

Fault sequences that could result in a URC or theft scenario are identified, and the claimed initiators and SSCs compared against the list of CBSIS associated with those SSCs, in order to determine which CBSIS elements contribute to the identified fault sequences.

32.7.4.2 Step 2 – System Identification

The identified CBSIS and CBSy are subject to initial screening and categorisation. The intent of this step is to screen out systems that are not vulnerable to cyber-attacks due to their implementation technology.

For systems that are vulnerable to cyber-attack, this step defines the system boundaries, interconnections and support systems, and allows assignment of a security degree to each system. This activity is part of the preliminary assessment activities from a SbyD perspective. CBSy elements will also be assigned a security classification / categorisation [47] which allows the assignment of an appropriate security degree.

The initial control set suites for Baseline and Security Degrees 1 to 3 have been developed based of relevant standards [48] & [49].

This initial assessment may identify potential vulnerabilities within the system under consideration such as interconnections, weaknesses due to maintenance access or support systems.

Consequences of CBSIS and CBSy compromise are based upon the worst-case consequences as detailed within the fault schedule, modified by the contribution of the CBSIS/CBSy to that fault sequence. Consequences of system compromise are then categorised against criteria presented within the SyAPs Annexes [16].

32.7.4.3 Step 3 – Initial Cyber Security Risk Assessment

An initial cyber security risk assessment is performed based on the initial concept design of the CBSIS and CBSy. An assessment of cyber risk is determined based upon the combination of consequences and likelihood of a successful attack using a defined risk matrix.

Each threat actor/attack method combination is considered separately to determine if:

- Such an attack is credible
- The attack can penetrate and compromise the CBSIS/CBSy under consideration.

Security benefit is only to be claimed for inherent system design features provided for operational or safety reasons. No claims are made on the addition of CBSy or other dedicated security features.

This initial risk assessment provides the following benefits:

- Risk scoring for all threat actor/attack method combinations for the system under consideration
- Identification of CBSIS systems with high levels of cyber risk that require significant security resources
- Identification of threat actor/attack method combinations that are not credible for the system under consideration

- Identification of CBSIS systems that through a combination of low compromise consequence and system design features, have an acceptable level of risk. Such systems are documented within the security case, assigned the baseline security control set and are not subject to further risk assessment – See Step 5 Tolerability of Risk

- Identification of vulnerabilities or potential design changes that will be included within the SbyD process

- Where credible threat actors are applicable to the CBSIS system, CPS outcomes can be assigned to each security sequence based on the skill level of the threat actor and the consequence of system compromise.

32.7.4.4 Step 4 – Zones and Conduits

Prior to a detailed risk assessment, the systems under consideration are subject to a formal zoning exercise to determine system security zones – based on a number of parameters. In addition, conduits into/from each zone are identified and the details of such conduits confirmed (for example, direction of communications, communication protocol/type, purpose of the communications).

This both simplifies the following detailed cyber security risk assessment by defining system boundaries and interfaces to be protected.

Zoning also supports the SbyD principle and the graded approach allowing control sets to be assigned by specific zonal requirements and providing separation and segregation between systems.

32.7.4.5 Step 5 – Tolerability of Risk

Based upon the initial risk assessment performed under Step 3, threat actor/attack method combinations, where the initial risk is within the risk appetite, are identified.

Such risks are considered to be tolerable, and no additional risk assessment is considered for these entries. A baseline security control set is assigned in accordance with IEC 63096 [49].

It may be possible that entire systems are deemed to have a tolerable risk due to a combination of credible threat actor/attack methods, technology choices, inherent design features and low compromise consequences.

Systems that have threat actor/attack method combinations that have higher than acceptable unmitigated risk levels are subject to detailed risk assessment (CSRAM Step 6).

32.7.4.6 Step 6 Detailed Cyber Security Risk Assessment Phase 1

The Detailed Cyber Security Risk Assessment is performed on those systems which due to a combination of threat actor/attack method, compromise consequence, and internal design features have an initial level of risk that is not acceptable. The intention is that detailed assessment is carried out on a design that has matured compared to that considered by the preliminary assessment.

Each threat actor/attack method combination is reviewed to determine its credibility, the extent of the compromise, and the potential for the attack to remain within the system or transfer to interconnected systems. The potential for the inherent design features to provide a security benefit is also considered.

An initial risk ranking is determined. Those threat actor / attack method combinations where the initial risk ranking is acceptable are documented. These threat actor / attack method combinations are assigned the baseline security control set and may also benefit from additional control sets implemented for other threat actor/attack method combinations for the system under consideration.

Threat actors are based on the threat information in [25] whilst both the STRIDE and Mitre Attack Methodologies detail potential initial attack methods. The Mitre Attack Methodology is also used to determine the cyber-attacks pathway through the system to critical components or to other systems. This pathway provides information to allow the placement of control sets (CBSy).

Phase 1 of the Detailed Cyber Security Risk Assessment allows the following:

- The identification of threat actor / attack method combinations where the unmitigated risk assessment has identified that the risk level is acceptable. Such sequences are documented and justified within the Generic Security Case, and subject to the application of baseline security control measures.
- The identification of valid threat actor / attack method combinations, which require mitigation either by additional design changes or the imposition of control sets that correspond to the system security degree.
- The identification of attack pathways through the system to allow placement of control sets / CBSy.

32.7.4.7 Step 6 Detailed Cyber Security Risk Assessment Phase 2

For those valid threat actor/attack method sequences which require additional mitigation, this phase identifies appropriate design changes to mitigate/remove the cyber security hazard. Where design changes are not possible, applicable control sets are specified.

Phase 2 of the Detailed Cyber Security Risk Assessment allows the following:

- The identification of CBSIS where security controls can be implemented to reduce risk to an acceptable level.
- The identification of CBSIS where security controls are insufficient to reduce risk to an acceptable level and design changes should be considered (via the SbyD Process).
- The identification and location of security controls for inclusion within the C&I design (via the SbyD process).
- The identification of potential security controls for consideration for their acceptability to the safety case.
- The determination of initial residual risk levels for consideration as to their acceptability within the safety case.

32.7.4.8 Step 7 Justification

Step 7 presents the conclusions derived from the cyber security risk assessments, including residual risk scores, cyber security design requirements, and assigned control sets. There will be a

deterministic justification that the residual risk levels are suitably low and acceptable; and that CPS outcomes have been achieved.

Design requirements and control sets developed within the cyber risk assessment process are transferred to the C&I Design Team for incorporation within the system design, and to the Safety Team for consideration within the safety case (both to confirm the cyber-risk levels do not compromise the safety case claims, and that the design requirements/control sets do not prejudice the safety functionality of systems claimed within the safety case).

The documented results of the cyber security risk assessment process provide evidence to support the CAE structure which demonstrates that security risks have been controlled and reduced to an acceptable level.

32.7.5 Multiple Systems

The defence in depth concept typical to Nuclear Power Plants ensures that multiple systems must fail in order to generate a significant radiological release. As such, the cyber security assessment must consider the cases where multiple CBSIS / CBSy must be compromised in order to generate a URC or theft event.

The nature of security assessment is restricted due to the lack of accuracy probabilities for the probability of attack and the potential uncertainties regarding attacker capabilities. This mandates a deterministic approach to multiplicative claims unlike the quantitative assessments associated with the safety approach.

Where multiple systems are required to be compromised, the base risk level for the combination of systems is the lowest risk level of the individual systems within the combination. An additional risk reduction level (for example Low to Very Low) can be claimed for each additional system subject to restrictions regarding the additional system risk level and dependencies between systems.

Where additional systems included in the combination have a significantly higher risk level than the lowest system risk level, then the security benefit of the 2nd system may not be claimed.

Where there are security dependencies between systems within the combination, the security benefit of the 2nd dependent system may not be claimed.

32.7.6 Integration with Secure by Design Approach

Application of the SbyD methodology [9] ensures that potential sources of security risk are identified and subsequently eliminated or reduced at source prior to the need to apply security measures.

Preliminary Assessment provides early security-informed input into the design process by building upon a number of assumptions and judgements prior to a formal application of the methodology. This supports early application of the SbyD principle at a time where the ability to influence the design is arguably at its greatest. Preliminary assessment from a cyber security risk perspective is discussed in the sub-section below.

The initial steps of the CSRAM (Steps 1 and 2) are triggered after an initial assessment of an engineering work package is undertaken within Stage 1 Step 1 of the SbyD Methodology [9]. The work packages are design activities that culminate into SSC design definitions. Identification of work packages goes through two steps:

- Stage 1 Step 1 of the SbyD Methodology is an initial assessment by the work package owner to determine if the package may be relevant to SbyD. This is facilitated through the provision of a questionnaire (based on flowchart in [9]. Answering 'Yes' to any question triggers a more detailed assessment by the security SQEP.

- Stage 1 Step 2 of the SbyD Methodology is a more detailed assessment by a security SMEs. The security-led assessment determines the inherent security risk present in the SSC and whether there is an opportunity to reduce the risk through SbyD. To do this the security SMEs initiate a preliminary assumption-based assessment (PAA) referred to as Steps 1 and 2 of the CSRAM [31].

Stages 2 and 3 of the SbyD Methodology are implemented during the detailed assessment phase of the CSRAM methodology (see sub-sections 32.7.4.6 and 32.7.4.7).

32.7.7 Outputs from Cyber Security Risk Assessment

In future Issues, this sub-section will summarise the outputs from the on-going application of the CSRAM, these include:

- The identified cyber risk

- The control sets identified through the CSRA.

It will then summarise how the SbyD Principle is being applied to design out vulnerabilities and the security control sets that are being designed into the system to match the CPS Security Outcomes, Postures and Responses (SOPRs) that are determine by the consequence of the loss of each system.

32.7.7.1 Critical Review of the CSRAM Methodology

Due to the early maturity of the DPS and RPS design, the Pilot Study undertaken for the CSRAM was not intended as a formal assessment. Rather, this was an opportunity to trial the CSRA and identify potential improvement.

The design maturity of the RPS and DPS only allowed indicative control sets to be determined within the scope of the trial. Subsequent assessments of the central control and safety systems (C&I) will define a complete set of control sets and reference will be provided back to the control sets and functionality detailed within Appendix A of the CSRAM [31].

A critical review [45] identified improvements that are being incorporated in the CSRAM.

32.7.8 Integrated Security Solution

The output from the CSRA is taken forward into the development of a CPS and PPS as part of the overall ISS. This is undertaken as part of the overall SbyD Approach. This work includes the identification of the Outcomes and Postures from the relevant SyAPs Annexes [16], which in turn identifies the requirements for the CPS.

32.7.9 Future Work

The learning from the CSRA Pilot Study identified meaningful improvements. These improvements will be incorporated a future up-issue of the methodology [31]; and, reflected, as appropriate, within an up-issue of the SbyD methodology [4].

In conjunction with the on-going initial stage of the SbyD approach, a schedule is under development for the more detailed application of the CSRA to the relevant CBSIS (and eventually CBSy). The schedule will be based around the following:

- Maturity of CBSIS or CBSy
- Plant Area – e.g. Reactor Island, Balance of Plant, Turbine Island
- Security Importance, e.g. Safety Cat A/Class 1.

The intention is that the detailed CSRA should be undertaken as CBSIS designs mature toward DR3. The application of CSRA falls under Stage 2 of the SbyD methodology. This allows for any design recommendations or requirements that arise to be incorporated as part of the design optioneering leading up to a FCD at DR3.

The application of the CSRA is not intended to be a one-off but rather an iterative process. For example, it would be repeated (post-DR3) if there were to be any significant changes in design [11] or changes to DBT or other threat intelligence.

32.8 Vital Area Identification and Categorisation

32.8.1 Introduction

The identification and categorisation of Vital Areas is applied to understand the vulnerability of the RR SMR to acts of sabotage that could result in an URC. This takes into account the direct application of the DBT or where the threats could be used in combination over a number of systems to lead to a URC.

The overall process for identifying and categorising Vital Areas comprises a series of interlinked assessments as shown in Figure 32.8-1.

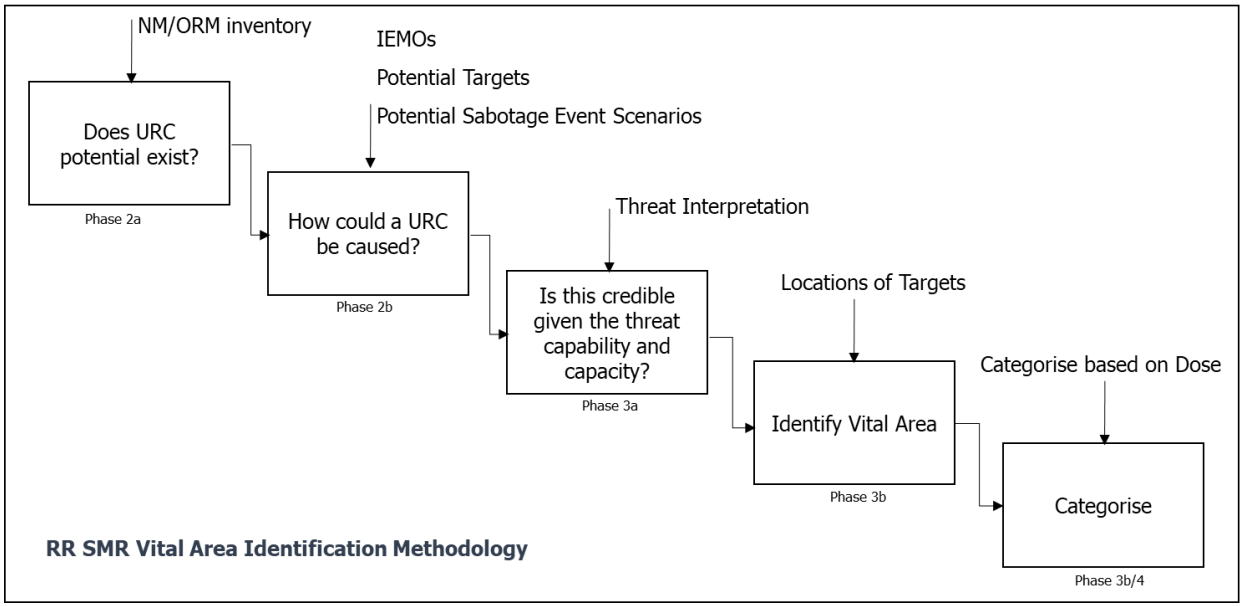


Figure 32.8-1: Vital Identification Process

A structured VAI&C methodology [7] has been developed in line with the RGP (both international and UK national).

This methodology identifies potential physical and cyber threats which could result in a URC. The methodology has been demonstrated through a pilot study [50] prior to its application across the RR SMR.

32.8.2 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to VAI&C.

More detailed CAE is presented in the most recent issue of the following Tier 2 report:

- Rolls-Royce SMR: Vital Area Identification and Categorisation Methodology [35]
- Rolls-Royce SMR: Vital Area Identification and Categorisation Report [51].

These Tier 2 documents reference Tier 3 sources of evidence, including that relating to the application of the methodology.

32.8.3 Claims Addressed

The relevant high level (Level 1) Nuclear Security sub-claim is:

[E3S Claim 32.4] Protection from Sabotage: The design basis threat of the sabotage of nuclear material or other radioactive material which could result in Unacceptable Radiological Consequence will be managed through the application of a Vital Area Identification and Categorisation (VAI&C) Methodology to identify requirements for proportionate security measures. These security measures will form part of an Integrated Security Solution (ISS) for the generic RR SMR.

This Level 1 sub-claim is supported by a set of Level 2 sub-claims, the intention of which is to link them with the various pieces of evidence which, when taken together, demonstrate that the Level 1 sub-claim is met. These Level 2 sub-claims are:

[32.4.1] A structured Vital Area Identification and Categorisation (VAI&C) methodology has been developed and applied in line with the relevant good practice (both international and UK national) for the identification of Vital Areas for the RR SMR. This methodology identifies potential physical and cyber threats which could result in an Unacceptable Radiological Consequence (URC).

[32.4.3] The security solutions to address the sabotage risk (from physical, cyber or blended attack) to the identified Vital Areas are developed and included with the Integrated Security Solution (ISS) for the generic RR SMR.

[32.4.2] The vulnerability to sabotage of SSCs (as a result of a physical, cyber or blended attack) have been reduced through the application of Secure by Design. This has resulted in the minimisation of the scope and number of Vital Ares (and where practical) a reduction in the categorisation of such.

These sub-claims are tabulated in Appendix D (Section 32.17), which also presents and further decomposition to Level 3.

32.8.4 Vital Areas - Definitions

A Vital Area is defined as an area containing NM/ORM (including radioactive sources), or equipment, systems, structures or devices, the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant DBT, could directly or indirectly result in unacceptable radiological consequences, thereby endangering public health and safety by exposure to radiation as outlined in SyAPs [7].

A URC is the radiological consequences of sabotage that exceed the classified UK radiological dose threshold outlined in SyAPs. This includes all pathways over a 24-hour period at the facility perimeter. This dose is assessed on an unaverted basis (assuming no implementation of countermeasures during the 24-hour period) unless there are strong reasons for assessing the dose on an averted basis.

Doses above the classified URC threshold are separated into two regions by a second, higher, radiological dose level. Locations associated with sabotage actions which do not yield a radiological dose in excess of the lower URC threshold are not Vital Areas and are defined as Baseline.

Targets, which if successfully sabotaged, can yield a radiological dose in the upper URC region, are referred to as High Consequence Vital Areas (HCVAs) whereas those which yield a radiological dose above the URC threshold but below the HCVA lower threshold are referred to as Vital Areas (VA) as shown in Table 1. Areas containing NM/ORM whose sabotage does not lead to a URC are still identified as they need security protection (against theft) as Baseline Areas.

Table 32.8-1: Categorisation of Vital Areas

Radiological Dose Region	Categorisation
> Upper URC Threshold	HCVA
Lower URC Threshold < > Upper URC Threshold	VA
< Lower URC Threshold	Baseline Area

32.8.5 Overview of the VAI&C Methodology

The methodology process for VAI&C is focused on the inventory at the SMR site which has the capability of leading to a URC if sabotaged. Once the inventory is established it is then determined if and how a URC can be caused. This process takes account of the capability of the threat to cause a URC.

The VAI&C process also integrates with the safety engineering team by ensuring that any identified hazards resulting from the analysis is recorded in the project wide Hazard Log. As well as the Hazard log being a potential input location for VAI&C outcomes, it is also be utilised as an input source to initiate the VAI&C process when necessary.

Figure 32.8-2 presents the overall VAI&C methodology stages from Phase 0 to Phase 4.

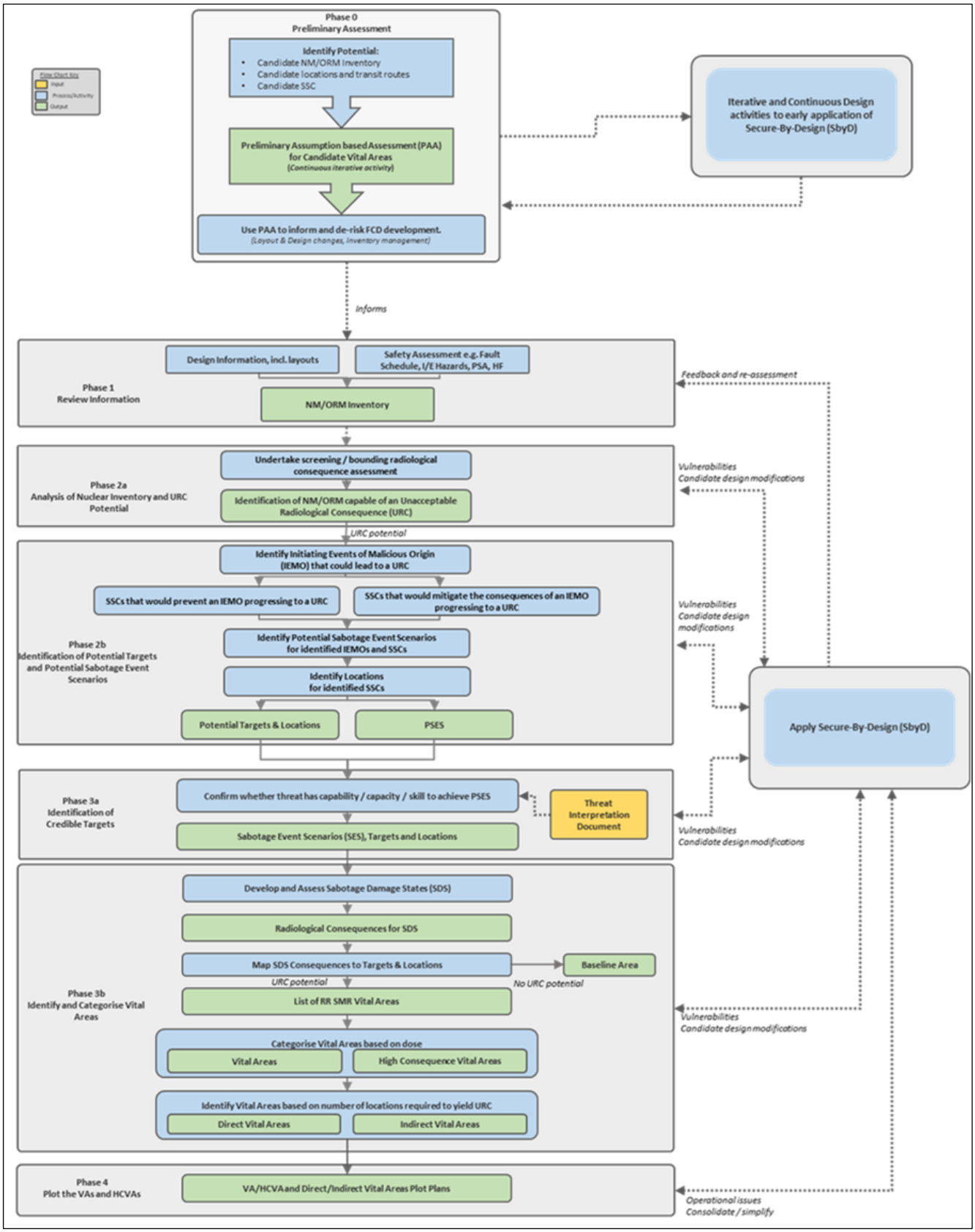


Figure 32.8-2: Overall Vital Area Identification and Categorisation Methodology

32.8.5.1 Phase 0 – Preliminary Assumption-based Assessment

Phase 0 provides early security-informed input into the design process by building upon a number of assumptions and judgements prior to a formal application of the methodology. This supports early application of the SbyD principle at a time where the ability to influence the design is arguably at its greatest.

Application of the SbyD methodology ensures that potential sources of security risk are identified and subsequently eliminated or reduced at source prior to the need to apply security measures. Phase 0 of VAI&C is applied after an initial assessment of an engineering work package is undertaken within Stage 1 Step 1 of the Secure by Design Methodology [9].

32.8.5.2 Phase 1 – Analysis of NM/ORM Inventory

Phase 1 forms a preparatory stage where information is gathered to prepare for a formal application of the VAI process, Phases 2 to 4. During this phase, a team is established, and information is sought to support the process. The NM/ORM inventory is obtained, reviewed and/or compiled to support the study. In the event that information gaps are identified, justified assumptions may be made and recorded to enable the assessment to proceed.

Once all the prerequisite information and inventory detail is gathered, the methodology moves to the next phases.

32.8.5.3 Phase 2 – Identification of IEMOs, PSESs, Potential Targets and Their Locations

Phase 2a is an assessment made to determine which parts of the inventory have the potential to give rise to a URC if successfully sabotaged.

Phase 2b considers the inventory identified with URC potential in Phase 2a and follows a structured process to determine the means by which a URC could be released by acts of sabotage. This includes both direct sabotage of the NM/ORM itself and combinations of acts which could cause the loss of the Fundamental Safety Function (FSF) which is keeping the NM/ORM in a safe state.

The SSCs which would require sabotage for the URC to be released are identified as Potential Targets and their locations identified. Combinations of sabotage-related failures, termed Potential Sabotage Event Scenarios (PSESs) at this stage are derived to inform subsequent phases of the assessment.

32.8.5.4 Phase 3 – Identification of Credible Sabotage Damage State (SES) and Targets

Phase 3a applies the threat interpretation (derived separately) which outlines the capability, capacity and skill level of the threat to the Phase 2b assessment to confirm (or otherwise) if the combinations of events identified in Phase 2b are credible for an attack group to achieve. Credible combinations are termed as Sabotage Event Scenarios (SESs) and the Potential Targets within them are identified as Targets. The SESs are taken forward for further assessment in Phase 4

Phase3b outlines the final damaged state of the plant and an assessment of the radiological consequences of a release for each credible SES is undertaken. Vital Areas are identified and categorised for the locations of each Target to support the subsequent development of potential security measures.

32.8.5.5 Phase 4 Identification and Categorisation of Vital Areas

The identified Vital Areas are categorised based on the magnitude of the potential radioactive release. The identified and categorised Vital Areas are then plotted on floor plans to provide a visual representation of the RR SMR Vital Areas to complete the VAI&C methodology for the engineering work package in question. The work package is then managed through the SbyD modification process where required.

32.8.6 Outputs from VAI&C

In future issues of the GSR, this sub-section will summarise the output from the application of the VAI&C methodology to the relevant SSCs which make up the RR SMR.

Phase 0 interactions between security SMES and design engineers continue to be on-going. Typically, these are occurring as a SSC design maturity nears DR1. It is recognised that the process for this interaction (primarily a part of Stage 1 of the SbyD methodology) would benefit from a more formalised approach. Additionally, the traceability of evidence from these interactions also requires improvement.

The methodology has been applied in full only in the form of a pilot study. This pilot study as undertaken for the Fuelling Block [51] & [50]. At the time of the Pilot Study the design maturity was post-DR1 but pre-DR3; that is various design options where being identified and tested prior to final selection.

The outputs from the Pilot Study [51] & [50] included:

- Potential design options to reduce vulnerability to sabotage
- Recommendations for improvements to the VAI&C methodology and its further integration within the SbyD approach.

32.8.7 Integrated Security Solution

The output from the VAI&C methodologies (for example required Outcomes and Postures) is taken forward into the development of a PPS and CPS as part of the overall ISS. As part of the development of the ISS, the security functions which deliver these Outcomes and Posture is assigned to security SSCs. This is undertaken as part of the overall SbyD Approach.

32.8.8 Future Work

The learning from the application of Phase 0 and the VAI&C Pilot Study has identified improvements, which will be incorporated a future up-issue if the VAIC methodology [35]; and, reflected, as appropriate, within an up-issue of the SbyD methodology [9].

In conjunction with the on-going Phase 0 interactions, a schedule is under development for the more detailed application of the VAI&C methodology to the relevant SSCs. The schedule will be based around the following:

- Maturity of SSCs
- Plant Area – e.g. Reactor Island, Balance of Plant, Turbine Island

- ‘Security Importance’, e.g. presence of NM, Safety Cat A/Class 1.

The intention is that the Phase 1 to 4 of the methodology should be applied initial as an SSC design matures toward DR3. The application of Phases 1 to 4 fall under Stage 2 of the SbyD methodology. This allows for any design recommendations or requirements that arise to be incorporated as part of the design optioneering leading up to a FCD at DR3.

The application of the VAI&C methodology is not intended to be a one-off but rather an iterative process. For example, it would be repeated (post-DR3) if there were to be any significant changes in design [37].

32.9 Integrated Security Solution

32.9.1 Introduction

The SbyD approach (see Section 32.5) adopted for the RR SMR promotes the integration of Physical and Cyber Protection Systems (PPS & CPS). Further to this the adoption of SbyD at the initial stages of the design process provide an opportunity to influence the design to reduce security vulnerabilities (and lessen the requirements for the PPS and CPS).

This Section summarises how Rolls-Royce SMR Limited is applying a holistic approach to development of the security solution for the RR SMR, bring the PPS & CPS together in an Integrated Security Solution (ISS).

The primary objectives of the ISS are to provide a future Operator with:

- A full understanding of the security solution for the RR SMR and how it has been developed
- The assumptions inherent in the ISS and what Operator owned risks need addressing
- The basis for the development a Nuclear Site Security Plan (NSSP) (in UK) or similar (worldwide).

The development of the ISS adopts an iterative approach, which is achieved through a Systems Engineering approach that is compliant with the relevant Rolls-Royce SMR Limited engineering processes.

Primarily, the ISS protects against theft of nuclear or other radioactive material and sabotage, which could result in an unacceptable radiological consequence. The ISS also takes account of business risk, for example the loss of operation due to malicious incidents.

By understanding how the ISS has been developed, why security functions and measures have been selected and their links to the E3S case, it is possible to derive a security plan for an operational RR SMR. This security plan presents how the security case meets the regulated outcomes, and how it considers business outcomes, in all operational states and throughout the lifecycle of the plant.

32.9.2 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to the development of the ISS into a site security plan.

More detailed CAE is presented in the most recent issue of the following Tier 2 report:

- Rolls-Royce SMR: Integrated Security Solution [12].

This Tier 2 document references Tier 3 sources of evidence, including that relating to the design of security SSCs.

32.9.3 Claims Addressed

The relevant high level (Level 1) Nuclear Security sub-claim is:

[E3S Claim 32.5]: The Integrated Security Solution (ISS) has been developed for the generic RR SMR. The ISS provides future Operators with a full understanding of the security solution and how it has been developed; and provides the basis for the subsequent development of a security plan for an operational RR SMR which will both meet regulatory expectations for nuclear security and address the commercial risk appetite of the Operator.

This Level 1 sub-claim is supported by a set of Level 2 sub-claims, the intention of which is to link them with the various pieces of evidence which, when taken together, demonstrate that the Level 1 sub-claim is met. These Level 2 sub-claims are:

[32.5.1] The Integrated Security Solution (ISS) is based around security infrastructure which provides for both a Physical Protection System (PPS) and a Cyber Protection System (CPS). The framework for the development of the security infrastructure ensures that it is integrated into the plant design to provide a holistic security approach for the generic RR SMR.

[32.5.2] The Integrated Security Solution (ISS) provides the basis for a security plan for an operational site, that is a Nuclear Site Security Plan (NSSP) for a UK deployed RR SMR or similar under other national regulatory regimes.

These Level 2 sub-claims are further decomposed as outlined in the relevant sections of this document and summarised in Appendix E (Section 32.18).

Rols-Royce SMR recognises that the current claims structure of the ISS requires further rationalisation and development.

32.9.4 Philosophy of ISS

Historically, nuclear security requirements for nuclear power plant (NPP) were prescribed by the relevant regulatory authority. Over the last decade there has been a transition from a prescriptive based approach for civil nuclear security regulation, to an outcome-focused model, where the Operator has greater freedom in the design of the security solution.

Following the issue of the ONR SyAPs [7], the regulatory regime for nuclear security in the UK has become more permissive. Dutyholders are now required to meet certain Security Outcomes and Postures [16]. These outcomes are determined from the results of security analyses undertaken to assess risk of sabotage, theft (of NM and/ORM) and cyber-attack. Typically, analysis was undertaken on a final (or near complete) engineering design for a NPP.

The resultant security solutions typically comprised a PPS and a CPS which were “add-ons” to the engineering design, not part of it. The PPS and CPS were integrated to the extent that there was physical protection of cyber systems.

With increasing use of digital control systems and an ever more sophisticated cyber threat, the requirements for CPS have grown, including the necessity to protect the CPS both virtually and physically. This, together with an increasing threat from blended attacks (combined physical and cyber-attacks), has driven the increasing integration of the PPS and CPS.

The SbyD approach [9] adopted for the RR SMR includes for the integration of a PPS and CPS. Further to this the adoption of SbyD at the initial stages of the design process provide an opportunity to influence the design to reduce security vulnerabilities (and lessen the requirements for the PPS and CPS) and increase resilience.

The ambition is to develop a (truly) integrated solution; in which security is embedded into the design and future operation of the RR SMR.

An additional, but important aspect of the RR SMR ISS, is that it is constructed in a way that allows aspects of the solution (for example, measures, assumptions, and risks) to be tracked back from a security plan (developed from the ISS), through the ISS, to the PPS/CPS, and through the analysis undertaken, and ultimately to the design decisions taken to establish the security of the RR SMR.

32.9.5 Approach to the Development of the ISS

32.9.5.1 Scope of ISS

The ISS provides the basis to demonstrate how the relevant Regulatory Outcomes [16] are met within the RR SMR generic design.

The following security analyses are applied to the RR SMR design to identify potential vulnerabilities and areas where an improved design can be made inherently secure:

- Categorisation for Theft [33]
- Cyber Security Risk Assessment [31]
- Vital Area Identification & Categorisation [51].

Regulatory Outcomes are concerned with preventing the significant off-site release of radioactivity. These Outcomes (and associated Postures) are achieved through the designation of security functional requirements and the design of the SSCs which provide these functions. How these outcomes are achieved is recorded in the requirements management system [3].

Whilst those security measures which protect against significant off-site release also protect against threats to the commercial operation of a RR SMR, there may be other additional measures that could be taken to contribute to economic resilience.

Integration

The ISS is an overall solution which integrates the security measures which provide for physical and cyber protection; to ensure that they work as an integrated whole.

As noted above, the development of the ISS is integrated with the SbyD approach and engineering design. It can also be considered as a contributory part of an overall integrated E3S solution delivering the fundamental E3S objective for the RR SMR.

Furthermore, the ISS comprises a combination of

- Design features which provide a security benefit
- Identified design modifications which to seek to address security vulnerabilities and (ideally) remove or reduce such
- Dedicated security SSCs, that is SSCs whose primary purpose is address residual risk through the provision of security functions such as deter (for example, fences and other barriers), detect and assess (for example, cameras, alarms etc.) and delay (for example security doors).

Relevant Good Practice

Outside of the ONR SyAPs, RGP is available from other experience within nuclear and non-nuclear sectors. The IAEA provides an extensive series of information and guidance documents, chief amongst these being Infcirc/225 [13], broken down into:

- Nuclear Security Fundamentals, which establish the fundamental objective and essential elements of a State's national nuclear security regime
- Recommendations, which set out measures that States should take in order to achieve and maintain an effective regime
- Implementing Guides, which provide guidance on how States can implement the Recommendations
- Technical Guidance, which provide more detailed guidance on specific methodologies and techniques for implementing security measures.

Significant guidance and standards are available from the NPSA, via their extranet, from their Quarterly Threat Reports, Cyber Assurance of Physical Security Systems [34], Operational Requirements guidance [52] as well as their extensive range of guidance documents on all aspects of physical security (including the Catalogue of Security Equipment) and personnel security, e.g. on control rooms.

Advice and guidance on cyber related subjects are available from the NCSC, and publicly available through their website [53] including advice specifically applicable to industries that are part of the critical national infrastructure (CNI).

Non-nuclear standards, such the Loss Prevention Standards which are available from the Red-Book [54] may also be applicable to many areas, in particular where fire safety and security boundaries coincide, or where good commercial security is required, as opposed to nuclear security.

Security Analyses

As outlined in earlier sections, RR SMR has developed methodologies to assess the inherent security of the generic design through analysis for VAI&C, CfT and CSRA. The objective of these Rolls-Royce SMR Limited methodologies is to identify sensitive SSCs which require protection (by the ISS). SSCs include physical and digital systems, and software. These methodologies are applied iteratively as engineering design matures, allowing for security concerns to influence design. Vulnerability

assessment will ultimately demonstrate whether the design solution, including those inherent security features, achieve the necessary outcomes.

These analyses are applied in detail once the design of SSC is sufficiently mature. Typically, this is when an SSC approaches FCD at DR3. Up to DR3, SSC design is essentially optioneering and the influence of security requirements is recorded as part of this process [55].

It is these detailed analyses (typically at DR3 for SSCs) that identify the required outcomes that the ISS must meet in terms of protection of NM and ORM, SNI and sensitive SSCs. In identifying these outcomes, cognisance is taken of any security benefit inherent in the design or resulting modification identified by the preliminary assessments.

The iterative development of the ISS seeks to identify any further design modifications that assist in designing out vulnerabilities and contribute to achieving the required outcomes. Subsequent to DR3, a formal change control process [37] applies to any design modification proposed for the benefit of security. This change process addresses potential impacts on nuclear safety, operability, and other aspects impacting an SSC, of the proposed security modification.

Beyond this stage, the output from this system engineering process are the requirements for the integrated PPS and CPS to address the residual risk.

Equally, for design changes for reasons other than security, the GDA Security Team are advised and comment on such [37]:

- Where these changes are beneficial to security, due credit is taken within the ISS
- Where changes have a negative impact on security, these is discussed and, where possible, additional changes made to re-enhance, or mitigate these impacts.

Where re-enhancement or mitigation is not possible, the decisions around the change are recorded as part of the DR process [40].

Delivering for the Operator

The ISS provides a future Operator with:

- An understanding of how security case for the RR SMR has been developed, and the assumptions inherent in its design and development
- An understanding of how the RR SMR should be operated in order to comply with security case (Security Tech Specs) and the assumptions inherent in its operation
- The Operator owned risks to be addressed as part of its implementation.

The ISS comprises not just the security infrastructure provide by the PPS and CPS, but also include the security benefits that are inherent or included within the wider engineering design.

An understanding of these security benefits is critical for a future Operator, who must understand the security implications of altering the design or operation of the relevant SSCs. This would not be the case if the ISS relied solely on the PPS and CPS.

Due to the generic nature of the RR SMR design, assumptions are made on the commercial risk appetite of a future Operator/Dutyholder, and on how that Operator/Dutyholder will run the site. These assumptions are recorded as part of the ISS.

Based on the plant design, the security analysis and assumptions on risk appetite and operations, Security Tech Specs are produced and recorded in the ISS.

Due to the generic nature of the RR SMR design, some aspects cannot be adequately allowed for without the site-specific details. Equally, future technological developments in protective measures change to threats or regulation, or design changes originating from other E3S subject areas, might lead to recommended changes and alterations throughout lifecycle. Again, assumptions can be made about the nature of a site, and future technology changes, but there remains the risk that redesign may be necessary.

Maturity of Design

The scope and detail in the ISS are evolving as the engineering design of the RR SMR matures. Ultimately, the extent of and detail within the ISS depends on both overall Rolls-Royce SMR Limited Programme and Business Objectives (including security support offering) and the time and scope of individual customer engagement.

As a minimum (to support FCD for the RR SMR) a 'generic' ISS should comprise the following:

- Confirm the detailed requirements for the PPS & CPS and their main component sub-systems; upwards traceability of requirements or clear and agreed explanation for any gaps and why associated risk is acceptable
- Confirmation of the Categorisation of each significant facility, for theft and sabotage
- Confirmation of the agreed (with ONR) Security Outcomes and Response Strategy to be achieved for the facilities within each physical security zone, including CBSIS and critical Control and Instrumentation (C&I)
- An explanation of how the PPS and CPS deliver the Outcomes and Response Strategy
- Set out what the overall ISS comprises (for example, detailed definition of security zones, layout of Security Infrastructure)
- The categorisation of security functions and classification of security related SSCs
- Outline 'How to Operate' (including Security Tech Specs). That is how the security measures (PPS & CPS) and safety measures work in an integrated manner, and how those measures may be applied in the case of an escalating threat
- Where not already included within the design, requirements are sufficiently detailed to support detailed design of security SSCs (e.g. by a Security Integrator on behalf of Rolls-Royce SMR or future Operator)
- A full understanding of the security solution for the RR SMR and how it has been developed
- The assumptions inherent in the ISS and what Operator owned risks need addressing.

Preliminary Concepts

Ultimately, the detail of the ISS cannot start to be set out until the security analyses have been conducted in a meaningful way, as the Security Outcomes they generate are essential to allow effective development of the security solution.

The involvement of SbyD and the security analyses with the maturing engineering design provides sufficient understanding of the design, and its associated security vulnerabilities, for Security SMEs to establish a preliminary concept of the ISS.

This has several benefits, in particular:

- It allows for co-ordination between any proposed (security based) design modification
- Provides a starting point for the more detailed development of the ISS.

Such a preliminary concept is outlined in the ISS document [56]. At a high level, this concept provides an indication of potential security zones and the associated protective measures (PPS and CPS) that could be include in a more mature ISS.

32.9.6 Development of the Integrated Security Solution

32.9.6.1 Introduction

The development of the ISS adopts an iterative approach, whereby it seeks:

- To identify any design modification which can remove or reduce security vulnerabilities, such that the requirements for security measure necessary to address residual risks are minimised.
- Where further design modification is not possible, to identify and develop the required range of security measures which addresses the residual risks. That is the security measures that are delivered by the PPS and CPS.

This iterative approach is delivered through a systems engineering approach that is compliant with the relevant Rolls-Royce SMR Limited engineering processes.

It should be noted that this iteration of the ISS was undertaken following the declared RD 7 / DRP 1, as submitted in November 2023 [57].

32.9.6.2 Integrated Security Solution - A Roadmap

Figure 32.9-1 sets out (in diagrammatic form) a roadmap for the development of the ISS. This roadmap indicates the inputs into the ‘Systems Engineering’ which develops the ISS.

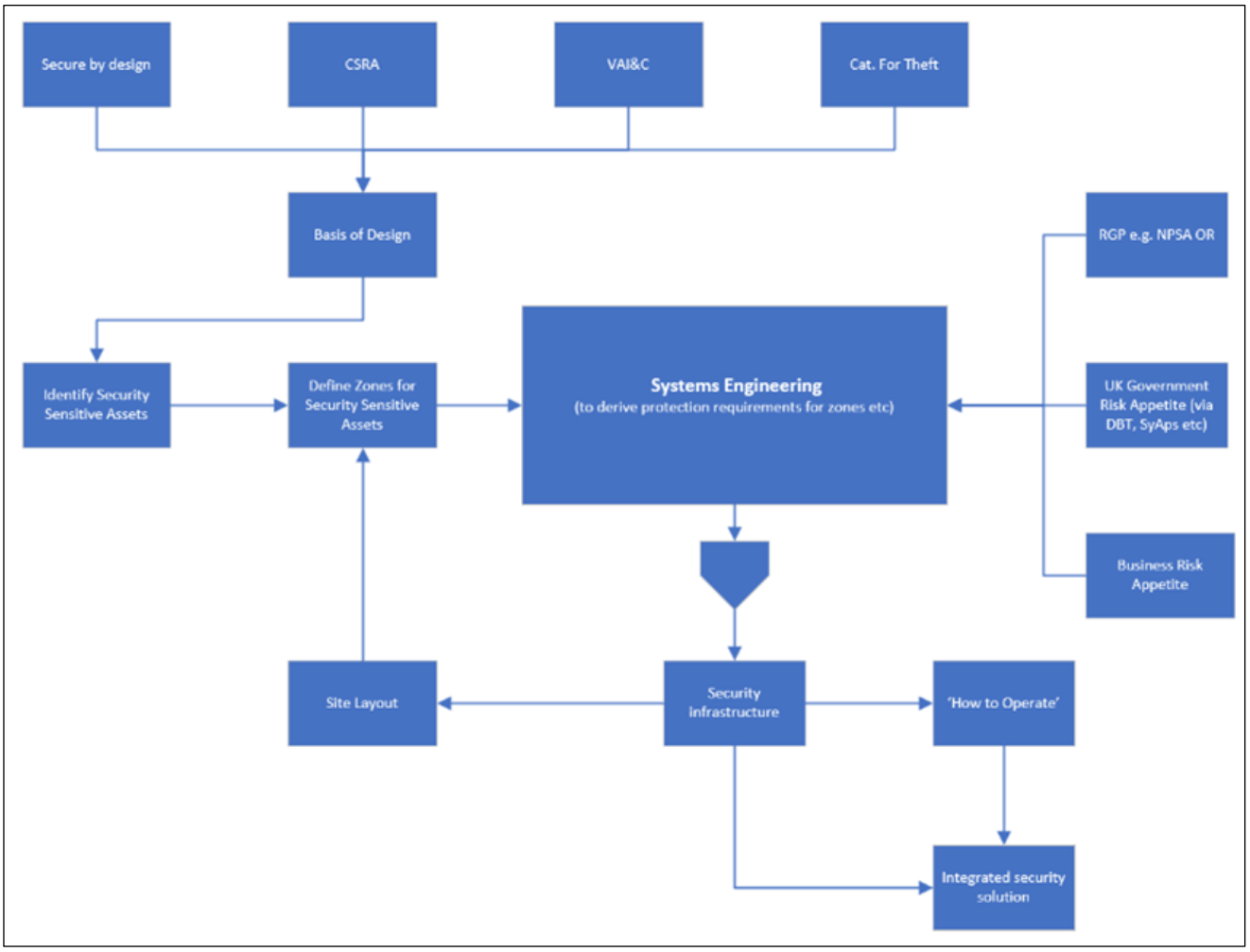


Figure 32.9-1: Integrated Security Solution (ISS) Roadmap

32.9.6.3 Systems Engineering Approach

The Systems Engineering Approach to the development of the ISS follows relevant Rolls-Royce SMR Limited engineering process, which includes:

- IMS Process C3.2.1-2, Definition Review (DR) process [40]
- IMS Process C3.2.2-3, Engineer safe, secure, safeguarded and environmentally sound products [32]
- IMS Process C3.2.2-2, Conduct design optioneering [55].

Further detail of the processes utilised are provided in the Tier 3 evidential documentation produced as the ISS matures. This could include E3S standards and engineering instructions on how security analyses and the design processes are integrated effectively.

The iterative process on Figure 32.9-2 comprises two loops which are as follows:

- An initial optioneering loop, which addresses the security measures which delivers the required Regulatory Outcomes (for a UK based RR SMR)

- A second optioneering loop, the intention of which is to identify any additional security measures needed to deliver the economic resilience of an operational RR SMR.

Figure 32.9-2: Systems Engineering Roadmap

Both loops seek to identify potential design modification and, ultimately, the security measures required to address residual risk. The latter are taken forward into the design of the PPS and CPS.

32.9.7 Further Development of the ISS

Security Requirements are input into the design through the E3S Requirements as described in the above document. As with all E3S Requirements, their incorporation into the design or justification of why they have not been accounted for is described as part of the DR process [40].

Company Standard Security and Safeguards Requirements and Analysis [58] is being prepared to describe the consideration of Security Requirements in the design. Additionally, the Standard describes the input of security requirements with respect to RGP, regulation and legislation relevant to the design process.

The requirements for both the PPS and CPS are based against analyses against the threat interpretation [25]. Future changes to the threat could require changes to the ISS (for example, on an operational RR SMR); this will be recognised within the PPS and CPS.

32.9.7.1 Physical Protection System (PPS)

Primarily, the PPS protects against theft of NM or ORM, sabotage (which could result in a URC) and the compromise of SNI. The assessment of this is against the threat interpretation [25]. The PPS also considers business security risks. Further to this, the PPS also considers protection of CBSIS and Computer-Based Security systems (CBSy).

The output from the relevant security analyses include:

- The scope and locations of NM and ORM and associated protective or mitigating SSCs (including OT and associated CBSIS) that should be protected by the PPS
- The Security Outcome to be delivered by the PPS, and that this degree of protection is proportionate to the risk.

Through the engineering process, the requirements are identified for a PPS which address the residual physical security risk.

In subsequent issues of this document, this Section will provide a summary of the PPS that has been developed as part of the ISS for the RR SMR.

Physical Security Functions

Physical security functions to meet the Outcomes are developed as the RR SMR design matures. The allocated functions are recorded in the requirements management database [3], which provide traceability from these functional requirements to the finalised security solution.

Specific details of security functions will be included in future issues of the ISS. Typical security functions for the PPS are introduced in sub-section 32.3.4

The ONR TAGs on Functional Categorisation and Classification [22] Policing [59], the Civil Nuclear Constabulary [60] and the use of civilian guard forces [61] allow Rolls-Royce SMR Limited to understand the regulator's expectations in these areas.

The Security Function Categorisation & Classification methodology [47] is applied to SSCs to recognise components providing inherent security and to security specific functions and measures developed to mitigate residual risk. This methodology is discussed further in sub-section 32.5.8.

The Functional Security Categorisation and Classification Methodology [47] complements the more general E3S categorisation and classification methodology [30].

Physical Security Infrastructure

An indicative set of the security measures that comprise a typical PPS are provided in the ISS [56], which also gives an indication of the security function delivered by these measures.

Physical Security Zoning

This sub-section will set out the Security Zoning around which the PPS is based (with reference as appropriate to more detailed sources of evidence). The proportionality principle is applied to any area segregation work. The intent being to ensure the appropriate level of security whilst enabling effective plant operations.

Physical zoning of the plant is conducted after the analysis of its systems have identified those most critical to the safe operation of the RR SMR. The drivers behind the zoning are categorisation for sabotage, theft and protection of SNI. Typical zones include (in increasing order of protection) a limited access area, a protected area and a facility (which houses the protected targets).

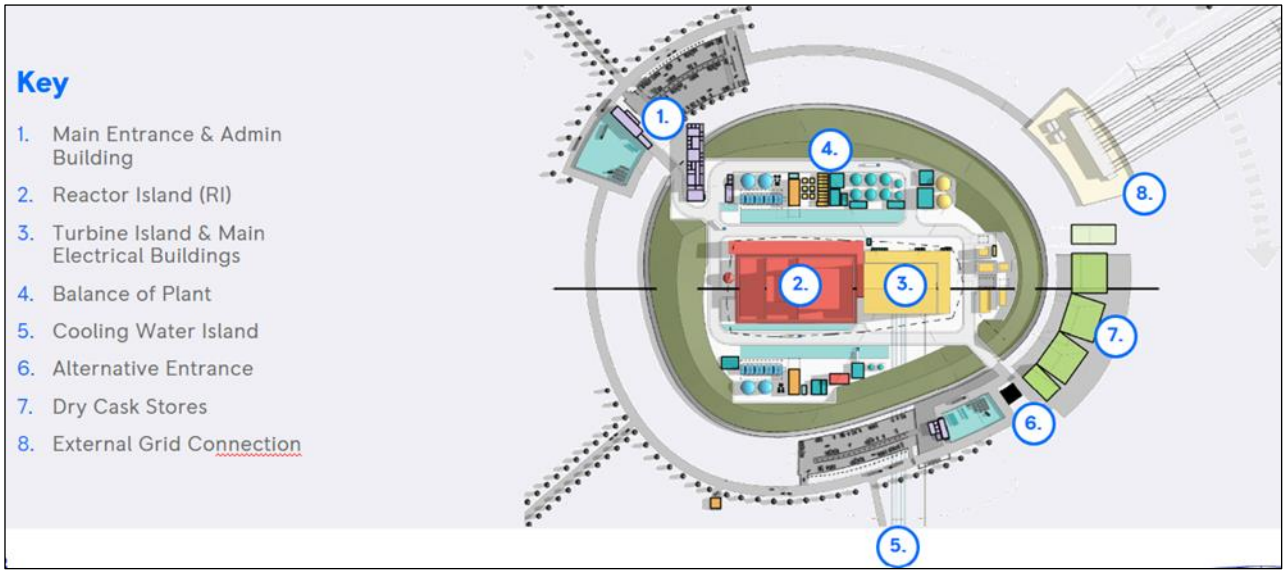


Figure 32.9-3: General Site Layout

Based on Figure 32.9-3, a preliminary identification of potential security layers or 'zones' outside the Reactor Island can be made:

- The outer site boundary is likely to be beyond the parking and vehicle lock areas and forms the first visible barrier. For example, this could be a fenced area delineating the Licenced Site showing designation as a Protected Place under the Serious Organised Crime and Police Act 2005 (SOCPA 2005).

- Within the outer site boundary, the next obvious zones are those bounded by the administrative building and berm. This includes a ditch and, potentially, double fencing, as well access control arrangements for vehicles and personnel.

The Reactor Island building itself forms a natural zone, with likely access control arrangements. This area can be further subdivided based on the following attributes:

- Access to Reactor Island
- The hazard shield; from a radiation protection perspective and a likely dividing line for NSV clearance requirements
- Safety & engineering systems (for example fluid & EC&I trains)
- Other systems such as the main control room, where only a limited number of personnel require access
- The Containment will be an area where access requirements will vary with the operating mode (for example, power production and outage periods).

Aspects Impacting an Operational PPS

The development of a PPS and how it operates is influenced by several factors. Some of these are practical considerations, such as space and power; others are driven by peoples' actions, or non-action. These include as follows [56]:

- Power & Space: Initial discussion on location and space requirements for the Security Control Centre (SyCC), and Emergency Response Centre (ERC), have been undertaken. Power requirements have yet to be defined. Power and space will also be required for the civil guard force and any on-site armed response force.
- Assumptions: During the development of security measures, assumptions are made on how they will be deployed, for example, based on determined worst case armed response times. These assumptions are based on legal requirements for the operator, relevant good practice and previous operator experience.
- Human Based Security Claims: Human Factors (HF) applies knowledge of human characteristics to optimise the design of products, equipment, environments, systems [62].
- Security Tech Specs: A Security Tech Spec is a procedure or action that must occur in order to remain within a secure operating envelope. That is, if the RR SMR was operated contrary to these Security Tech Specs the Dutyholder/Operator would also be in violation of the security case, and in the UK for example the NISR. Rolls-Royce SMR Limited will develop aspects of operations that are required for security measures, based on legal requirements, relevant good practise and the derivation of assumptions. These operational aspects are designated as Security Tech Specs within the security case.

32.9.7.2 Cyber Protection System

Primarily, the CPS protects against cyber attack against CBSIS and CBSy, with a potential to result in radiological release and/or compromise of nuclear safety systems, and compromise of SNI. The CPS also considers business risk.

The output from the relevant security analyses includes:

- The scope and locations of NM and ORM and associated protective or mitigating SSCs (including CBSIS & CBSy) that should be protected by the CPS

- The Security Outcome to be delivered by the PPS, and that this degree of protection is proportionate to the risk.

Through the engineering process, the requirements are identified for a CPS which addresses the residual cyber-security risk.

In subsequent issues of this document, this Section will provide a summary of the CPS that is being developed as part of the ISS for the RR SMR.

Cyber Security Functions

Cyber security functions to meet the outcomes are developed as the RR SMR design matures. The allocated functions are recorded in the requirements management system [3], which provides traceability from these functional requirements to the finalised security solution.

Specific details of security functions will be included in future issues of the ISS. Typical security functions are introduced in sub-section 32.3.4.

The Security Function Categorisation & Classification methodology [47] is applied to SSCs to recognise components providing inherent security and to security specific functions and measures developed to mitigate residual risk. This methodology is discussed further in Section 32.5.8.

The Functional Security Categorisation and Classification Methodology [47] complements the more general E3S categorisation and classification methodology [30].

Cyber Security Infrastructure

The CSRA methodology [31] currently calls for to the definition of a baseline set of cyber security controls for systems which, at the initial risk assessment stage are considered to have little consequence if they are compromised (that is, just basic cyber security to ensure confidentiality and availability).

The relevant standards [63], [64] & [65] identify controls that are either mandatory or optional depending on the system security degree and lifecycle phase.

The baseline set of security controls has been developed for the low consequence systems and systems with security degrees S1, S2 and S3. Rolls-Royce SMR Limited believes these suites of control sets are typical but are tailored to specific systems depending on system design and specific attack scenarios. An example of a potential baseline control set is provided in the ISS Tier 2 document [56].

32.9.8 Future Work

As the security analyses are completed the identified Outcomes and Postures (for both PPS and CPS) will be collated as the starting point for the design of the ISS.

32.10 Integration of Nuclear Security with Other Topic Areas

32.10.1 Introduction

The GSR forms Chapter 32 of the Integrated E3S Case; there are 33 chapters in total. The GSR is an integrated chapter within the E3S Case and the security assessment is not conducted in isolation. There is considerable interaction with other Topic Areas included within the overall E3S case. This integration involves both:

- Design engineers responsible for the various SSCs relevant to these topic areas
- The engineers responsible for the development Safety, Environmental and Safeguards cases (that is the topic areas covered by the individual chapters of the E3S Case.

32.10.2 Relevant Nuclear Security Claims

The relevant high level (Level 1) Nuclear Security sub-claim is:

[E3S Claim 32.1] Secure by Design: Security risk inherent in the design has been minimised through the application of secure by design principles and a credible secure by design methodology that integrates security considerations into the design process and security measures into SSCs, in a way that is consistent with the operational intent of the RR SMR, and before the application of dedicated security controls.

This Level 1 sub-claim is supported by lower-level sub-claims covering both SbyD and the ISS:

[32.1.1.1] Security risk inherent in the design has been minimised through the application of a credible secure by design methodology that includes security design principles and integrates security analyses and design activities into the engineering process, such that security risk is eliminated or minimised before the application of security controls, in a way that is consistent with the operational intent of the RR SMR.

[32.1.2.3] & [32.1.4.3] Recommended design changes have been screened for their impact to safety and operation of the RR SMR.

[32.1.5.1] Proposed security measured have been screened for their impact to safety and operation of the RR SMR.

[32.5.1.1.3] Deconfliction with safety requirements, environmental control measures and outage/maintenance activities, has occurred as part of the integrated E3S design process.

32.10.3 Future Work

Table 32.5-1 in Appendix F (Section 32.19) sets out the topic areas that are integrated with the security case and the high-level scope of interaction with these topic areas. This table is not exhaustive but intended to provide an indication of where the interaction is most important, based on RGP and ONR's Assessment Reports for Step 2. The interaction between the Security Case and

these other topic areas continues to grow as the engineering design matures and the E3S Case develops.

32.11 Development of a Site Security Plan

32.11.1 Introduction

The primary objective of the ISS is to provide a future Operator/Dutyholder with a full understanding of the security solution for the RR SMR and how it has been developed.

By understanding how the ISS has been developed, why security functions and measures have been selected and their links to the E3S case, it is possible to derive a security plan for an operational RR SMR.

Once derived, this security plan presents how the security case meets the regulated outcomes (and business risk appetite) in all operational states and throughout the lifecycle of the plant.

This Section discusses how the ISS can transform into a site security plan, which is the UK would be a NSSP, and highlights topic areas that need to be considered as part of this process.

32.11.2 Relevant Tier 2 and Tier 3 Evidence

This section of the GSR summarises the CAE relevant to the development of the ISS into a site security plan.

More detailed CAE is presented in the most recent issue of the following Tier 2 report:

- Rolls-Royce SMR: Integrated Security Solution [56].

This Tier 2 document references Tier 3 sources of evidence, including that relating to the design of security SSCs. Relevant Nuclear Security Claims

The relevant high level (Level 1) Nuclear Security sub-claim is:

[E3S Claim 32.5]: The Integrated Security Solution (ISS) has been developed for the generic RR SMR. The ISS provides future Operators with a full understanding of the security solution and how it has been developed; and provides the basis for the subsequent development of a security plan for an operational RR SMR which will both meet regulatory expectations for nuclear security and address the commercial risk appetite of the Operator.

This Level 1 sub-claim has been supported by a set of Level 2 sub-claims, the intention of which is to link them with the various pieces of evidence which, when taken together, demonstrate that the Level 1 sub-claim is met. The Level 2 sub-claims relevant to the topic of this Section is:

[32.5.2] The Integrated Security Solution (ISS) provides the basis for a security plan for an operational site, that is a Nuclear Site Security Plan (NSSP) for a UK deployed RR SMR or similar under other national regulatory regimes.

This Level 2 sub-claim is further decomposed as summarised in Table 32.18-1: Nuclear Security Sub-claims - Integrated Security Solution in Appendix E (Section 32.18).

32.11.3 Site Licensing - Lifecycle Considerations

32.11.3.1 Licensing

Once a site has been selected, site licensing activities start. Part of this is the production of a security plan, along with relevant supporting arrangements, and a separate security contingency plan (SCP). This plan should consider security during the upcoming phases of construction, commissioning, and operations.

This demonstrates to the relevant Regulatory Authority (the ONR for the UK) that adequate arrangements are being planned for the site to minimise the risk of the introduction of latent defects during construction and commissioning in such a manner that it could impact the safety of the reactor once operational.

32.11.3.2 Responsibility for Security Plan Production

It is the responsibility of the Operator/Dutyholder to produce security plans for all phases of a facility lifecycle. Rolls-Royce SMR Limited understands that these plans start from and relate back to the ISS.

Depending on the maturity of the customer, it is possible that Rolls-Royce SMR Limited might produce these plans. This would be advantageous to the Operator as the experience and knowledge gained during the ISS development can be exploited to produce an effective security plan.

32.11.3.3 Construction

Prior to the commencement of on-site activities in the UK, a Construction Site Security Plan (CSSP) must be approved by the ONR. As well as construction activities this plan should also cover the security governance arrangements for the site.

The CSSP should describe the security arrangements across all phases of construction, for example, ground investigations preparatory groundworks, installation of first nuclear safety components, bulk mechanical, electrical and heating, ventilation & air-conditioning (HVAC) installation, introduction of NM or ORM and first criticality.

Depending on the site, the CSSP also has to consider the impact of construction activities on neighbouring nuclear facilities, and the impact of the operations of neighbouring nuclear facilities on the construction site, particularly regarding emergency planning and response (EP&R).

32.11.3.4 Commissioning

During the run up to the first delivery of fuel to the plant there will be a shift of emphasis from construction security to nuclear site security. How this shift is managed will be articulated in future issues of the ISS to allow for the development of the CSSP.

32.11.3.5 Operations

Concurrent with the commissioning phase, in the UK, a NSSP will need to be written and approved by the ONR. This timing allows the site to transition smoothly from commissioning to operations.

The NSSP is the basis for security operations on an operational nuclear facility and is developed from the ISS. The NSSP has to consider all modes of operation of the plan.

32.11.3.6 Decommissioning & Demolition

The NSSP is adapted to a change in site operations as the plant comes to the end of its operating life. The NSSP must be maintained until the removal of the last NM or ORM, including and nuclear waste.

Knowledge of the original plan development from the ISS, assists future security personnel in deriving an effective security plan for the decommissioning and demolition phases.

Understanding how the risks were built up during design, development and construction assists in the further development of the NSSP during these phases of the site's life, up to the point where is no longer required.

32.11.4 Assumptions & Security Tech Specs

Assumptions and Security Tech Specs are developed as the ISS matures, in association with the identification of the security functions and design of security measures.

32.11.5 Emergency Planning & Response

The ISS accounts for not just the security measures designed into the RR SMR, but also how these are expected to function during an emergency. These measures and their operation should be included in the site-specific SCP.

Future issues of the ISS will expand on how secure measures are tested:

- For the PPS this may include what emergency arrangements need to be available, such as an emergency response centre, and how this interacts with the security control centre, as included in the control facility description document [66].
- The PPS arrangements should also consider the impacts to and from other adjacent or nearby nuclear facilities.
- The testing of any building or site lockdown arrangements needs to be included within the plan.
- Testing should consider all forms of attack, as specified in the design basis threat [25].
- Specifically for the CPS this should include such methods as penetration testing to assess for both malicious attack and accidental leakage or misuse.

Scope has been included within the RR SMR design to include an emergency response centre (ERC). This allows a coordinated response, across all disciplines, such as safety, environment, security (including physical & cyber), and the blue light services, to all incidents.

Consideration is also to be made for a Cyber–Security Operations Centre, to ensure adequate resource is available to tackle cyber-attacks and facilitate recovery afterwards.

The ONR has published relevant TAGs [67], [68] & [69]. These TAGs enable Rolls-Royce SMR Limited to understand the regulators expectations in these areas.

32.11.6 Site Specific Design and Risk

Once a site has been selected considerations have to be made for:

- Surrounding road infrastructure
- Potential site entry points (main or ancillary)
- Proximity of other nuclear facilities
- Landscape and potential areas of vulnerability or advantage within such, including the potential attack or reconnaissance points (e.g. for mortar or drone launch)
- Accessibility for emergency services, particularly an armed police service.

Such considerations are built into future issues of ISS, to allow subsequent inclusion in a CSSP and NSSP.

32.11.7 Ensuring the ISS Aligns with UK Regulation

Gap analysis is an important tool when producing a NSSP. To assist this future process, the ISS, will be mapped to the SyAPs [56]. This mapping highlights any shortcomings within the ISS against the expectations of the ONR, and also assist the ONR in assessing the completeness of the ISS.

32.11.8 Non-UK Regulatory Regimes

The CPPNM [10] places obligations on signatory states to protect nuclear facilities, and material in peaceful domestic use, in storage and in transit. The IAEA also provides guidelines for the protection of NM, though their Infcirc/225 [13], and the rest of the IAEA Security Series. Nation states adapt the obligations and IAEA guidance into legislative requirement though their own regulatory bodies.

Rolls-Royce SMR Limited will work closely with any national or regional bodies to understand their legislative requirements and adapt the development of the ISS into specific site security plans. Any security plan developed from the ISS will be aligned with specific national legislation, to ensure differing applications do not lead to gaps in the security plan.

32.12 Conclusions

32.12.1 Secure by Design

This Chapter outlines development of a Nuclear Security Case for the RR SMR. A SbyD approach has been adopted to promote the integration of security into engineering design, whereby security risk is evaluated and addressed at source, before considering any protection systems or mitigating features for the RR SMR.

The philosophy behind the Nuclear Security Case 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 a result of malicious acts.

This Chapter contributes to the overall structure of the E3S Case that facilitates the demonstration that the fundamental objective 'to protect people and the environment from harm' can be achieved at all lifecycle stages of the RR SMR, and demonstrate that risks can be reduced to ALARP, using BAT, and ensuring Secure by Design and Safeguards-by-Design.

This Chapter presents an overview of the security case as currently developed. The security case (as part of the E3S Case) is being developed alongside the ongoing design programme, as such the full suite of documentation / data that comprises the full case and underpin the claims made is still in development. The trajectory of arguments and evidence being generated, where known at this stage of the lifecycle, is documented in this chapter.

32.12.2 Assumptions, Commitments and Requirements

32.12.2.1 E3S Case

An essential element of the E3S Case development process is the capture and tracking of assumptions and commitments that are generated from the E3S Case, which need to be passed on to a future Dutyholder / Licensee / Permit Holder. These include matters such as Tech Specs, maintenance requirements, training programmes, or emergency preparedness. They are defined as:

- Assumption - statements that enable work to continue but need validation before they can be confirmed as true
- Commitment (or Requirement) - an assumed obligation on a future Operator / Dutyholder / Licensee / Permit Holder to conduct a specified activity

Assumptions and commitments are captured and logged in an 'Assumptions and Commitments for future Dutyholders/Licensee Register' in accordance with the Project Operating Instruction [70].

32.12.2.2 Security Case

Assumptions, commitments and requirements are recorded initially within the output from the application of SbyD and the supporting security analyses. These are taken forward into collated in the ISS prior to transfer into the E3S Register.

Full justification and explanation is captured in the ISS. The impact of deviation from such will also be indicated.

Future issues of this Chapter 32 will present a summary of the security related assumptions, commitments and requirements in this section.

32.12.3 Conclusions and Forward Look

The generic E3S Case objective at Version 2 is 'to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design' [1]. This confidence is built through development and underpinning of top-level claims across each chapter of the E3S Case, through supporting arguments and evidence. The top level claim for Chapter 32 is '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'.

The arguments and evidence presented to meet the generic E3S Case objective at Version 2 include SbyD Principles. These principles are established in the RR SMR requirements management system as non-functional system requirements, which are applied to design through engineering processes. The application of these processes supports the ongoing design of the RR SMR to minimise security risk and facilitate the integration of security into the overall design of the RR SMR.

Prior to completion of detailed security analyses (VAI&C, CfT & CSRA), the SbyD design approach has used these SbyD Principles, together with professional judgement and experience, to influence engineering design optioneering to reduce vulnerabilities; and hence reduce the scope and breadth of the security measures (as part of the ISS) that will provide protection against the residual risk. An example of this early interaction is the berm.

Further arguments and evidence to underpin claims will be developed in line with the E3S Case Route Map [71]. and reported in future revisions of the generic E3S Case, which will further build confidence that the RR SMR can deliver its fundamental E3S objective.

This Chapter demonstrates that the framework for SbyD has been developed and how it will continue to be implemented as the security analyses are undertaken. The results of these analyses will be presented in future issue of the relevant Tier 2 reports [35], [42] & [44]; and summarised in future issues of this Chapter. Only once these security analyses have been completed will the Outcomes and Postures that the ISS must deliver be identified; and specific detailed requirements for security measures derived. The programme for these security analyses is currently being finalised; with priority based around a combination of the following criteria:

- Security Significance (for example, the presence of NM/ORM, Category A Safety Systems)
- Plant Area (for example, Reactor Island)
- Design Maturity (for example, is this sufficient to allow for a meaningful analysis)

The ISS forms the basis for a future NSL for an operational RR SMR. The development of the ISS is summarised in Section 32.9 (of this Chapter), with more detail provided in the relevant Tier 2 document [56].

32.13 References

[1] Rolls-Royce SMR Limited, SMR0004294, Issue 3, “Environment, Safety, Security & Safeguards Case Version 2, Tier 1, Chapter 1: Introduction,” May 2024.

[2] Rolls-Royce SMR Limited, SMR0002183, Issue 2, “Rols-Royce SMR Generic Design Assessment Scope,” January 2023.

[3] Rolls-Royce SMR Limited, “DOORS Database /00_Small Modular Reactor/98 - Integration/00 - Architecture/SMR PBS Version 2.19,” December 2023.

[4] Rolls-Royce SMR Limited, SMR0004293 Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 33: Safeguards,” May 2024.

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

[6] His Majesty's Government, SI 2003/43, “The Nuclear Industries Security Regulations 2003,” Available: https://www.legislation.gov.uk/uksi/2003/403/contents/made, 2003.

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

[8] Rolls-Royce SMR Limited, SMR0004542, Issue 3, “Environmentt, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 2: Generic Site Characteristics,” May 2024.

[9] Rolls-Royce SMR Limited, SMR0005789, Issue 2, “Rolls-Royce SMR: Secure By Design Methodology,” May 2023.

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

[11] United Nations, “International Convention for the Suppression of Acts of Nuclear Terrorism,” 2005.

[12] “International Atomic Energy Agency Nuclear Security Series No 34-T,” Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control.

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

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

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

[16] Office for Nuclear Regulation, Security Assessment Principles for the Civil Nuclear Industry, Official Sensitive Annexes, Version1.1, 2022 Edition.

[17] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-6.1, Issue 2, “Categorisation for Theft,” March 2023.

[18] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-6.2, Issue 2, “Categorisation for Sabotage,” June 2023.

[19] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-GD-7.1, Issue 2, “Effective Cyber Security and Information Assurance,” March 2023.

[20] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-11.4.1, Issue 1, “Secure by Design,” January 2023.

[21] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-11.4.2, Issue 1, "The Threat," April 2022.

[22] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-GD-11.4.5, Issue 1, "Functional Categorisation and Classification of Security Structures, Systems and Components," April 2022.

[23] Rolls-Royce SMR Limited, SMR0001603, Issue 3, "Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles," August 2022.

[24] Nation Protective Security Authority, "NPSA Extranet - Threat Reports," 2024. [Online]. Available: https://extranet.npsa.gov.uk/threats/threat-reports.

[25] Rolls-Royce SMR Limited, SMR0006502 Issue 1, "Rolls-Royce SMR: Interpretation of Design Basis Threat (DBT) for the Generic Rolls-Royce SMR," February 2024 [SECRET].

[26] Rolls-Royce SMR Limited, SMR0009049, Issue 1, "Rolls-Royce SMR: Secure by Design Analysis," 2023.

[27] United States Nuclear Regulatory Commision, "US Code of Federal Regulations(CFR) Title 10, Part 73.1," 2022.

[28] Rolls-Royce SMR Limited, SMR0009697, Issue 2, "Rolls-Royce SMR: Secure by Design Report," February 2024.

[29] RR Report EDNS01000760628, Issue 2, "Secure by Design - Guidance Document - Principles and Method," 2020.

[30] Rolls-Royce SMR Limited, SMR0006518, Issue 1, "Rolls-Royce SMR Environment, Safety, Security and Safeguards Categorisation and Classification Methodology," July 2023.

[31] Rolls-Royce SMR Limited, SMR0006431, Issue 2, Rolls-Royce SMR: Cyber Security Risk Assessment Methodology, October 2023.

[32] Rolls-Royce SMR Limited, IMS Process C3.2.2-3, Engineer safe, secure, safeguarded and environmentally sound products, June 2022.

[33] Rolls-Royce SMR Limited, SMR0006854, Issue 1, "Rolls-Royce SMR: Categorisation for Theft Methodology," July 2023.

[34] National Protective Security Authority, "Cyber Assurance of Physical Security Systems Guidance," September 2022.

[35] Rolls-Royce SMR Limited, SMR0006499, Issue 1, "Rolls-Royce SMR: Vital Area Identification & Categorisation Methodology," June 2023.

[36] National Protective Security Authority, "STaMP Surreptitious Threat Mitigation Process," 2021.

[37] Rolls-Royce SMR Limited, IMS Process, C3.2.1-9, "Manage Change," March 2023.

[38] Rolls-Royce SMR Limited, IMS Process C3.1.1, "Define and Manage Requirements," 2022.

[39] Rolls-Royce SMR Limited, SMR0008573, Issue 1, "Environment, Safety, Security and Safeguards (E3S) Requirements and Analysis Arrangements," November 2023.

[40] Rolls-Royce SMR Limited, IMS Process C3.2.1-2, "Definition Review Process," September 2022.

[41] Rolls-Royce SMR Limited, SMR0008886, Issue 1, "Rolls-Royce SMR: Theft of Material & Categorisation Analysis," November 2023.

[42] Rolls-Royce SMR Limited, SMR0009686, Issue 1, "Rolls-Royce SMR: Theft of Material and Categorisation Report," January 2024.

[43] His Majecty's Government, "The Energy Act 2004 (as amended)," www.legislation.gov.uk/ukpga/2004/20/part/1/chapter/3.

[44] Rolls-Royce SMR Limited, SMR0008887, Issue 1, "Rolls-Royce SMR: Cyber Security Risk Analysis Trial," November 2023.

[45] Rolls-Royce SMR Limited, SMR0009698, Issue1, “Rolls-Royce SMR: Cyber Security Report,” January 2024.

[46] British Standards Insitute, “BS EN IEC 62443-3-2, Security for industrial automation and control systems Part 3-2: Security risk assessment for system design,” April 2023.

[47] Rolls-Royce SMR Limited, SMR0005655, Issue 2,, “Rolls-Royce SMR: Functional Security Categorisation & Classification Methodology,” October 2023.

[48] British Standards Institute, IEC62645, “Nuclear Power Plants- Instrumntation, Control and Electrical Power Systems - Cyber Security Requiremnts,” 2020.

[49] British Standards Institute, “BS EN IEC 63096 Nuclear power plant instrumentation, control and electical power systems - Security Controls Edition 1.0,” October 2020.

[50] Rolls-Royce SMR Limited, SMR0008452, Issue 1, “Rolls-Royce SMR: Vital Area Identification and Categorisation Analysis,” October 2023.

[51] Rolls-Royce SMR Limited, SMR0009689, Issue 1, “Rolls-Royce SMR: Vital Area Identification and Categoristation Report,” January 2024.

[52] National Protective Security Authority, “Operational Requirements Guidance,” 2018.

[53] National Cyber Security Centre, “Advice and Guidance,” [Online]. Available: https://www.ncsc.gov.uk/section/advice-guidance/all-topics. [Accessed 2024].

[54] L P C, “RedBook Live,” [online] avaiable https://www.redbooklive.com/.

[55] Rolls-Royce SMR Limited, IMS Process, C3.2.1-9, “Conduct design optioneering,” November 2022.

[56] Rolls-Royce SMR Limited, SMR0009908, Issue 1, “Rolls-Royce SMR: Integrated Security Solution,” February 2024.

[57] Rolls-Royce SMR Limited, SMR0009005, “Certificate of Design,” November 2023.

[58] Rolls-Royce SMR Limited, SMR0009104, Issue 1, “ SMR-STD-057, Security & Safeguards Requirements and Analysis,” April 2024.

[59] Office for Nuclear Regulation, Technical Assessment Guide, CNC-TAST-GD-9.1, Revision 1, “Local Police Forces,” March 2020.

[60] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-GD-9.1, “CNC Response Force,” March 2020.

[61] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-D-9.3, “Security Guard Services,” 2020.

[62] Rolls-Royce SMR Limited, SMR0004520, Issue 3, “Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 18: Human Factors,” May 2024.

[63] British Standards Institute, “IEC 62645, Nuclear Power Plants - Instrumentation, Control & Electrical Power Systems - Cyber Security Requirements,” 2020.

[64] British Standards Institute, “IEC 62443-3-3, Industrial Communications Networks - Network & System Security - Part 3-3: System Security Requirements & Security Levels,” 2013.

[65] British Standards Institute, “BS EN IEC 63096, Nuclear Power Plant Instrumentation, Control & Electrical Systems - Security Controls,” 2020.

[66] Rolls-Royce SMR Limited, SMR0005883, Issue 2, “Rolls-Royce SMR Control Facilities Descripition,” 2023.

[67] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-6.5, “Adjacent or Enclave Nuclear Premises,” 2022.

[68] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-GD-10.1 Revision 2, “CT Measures EP&R Planning,” October 2020.

[69] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-GD-7.5, Issue 4, “Prepartaion for and Response to Cyber Security Incidents,” January 2024.

[70] Rolls-Royce SMR Limited, SMR0002119, Issue 1, “Identifying, Recording and Tracking, GDA and Licensing Assumptions and Commitments,” 2023.

[71] Rolls-Royce SMR Limited, SMR0002155, Issue 3, “E3S Case Route Map,” 2023.

32.14 Appendix A: Nuclear Security Sub-claims - Secure by Design

The Secure by Design approach is the subject of a Level 1 security specific E3S sub-claim, as follows:

- [E3S Claim 32.1] Secure by Design: Security risk inherent in the design has been minimised through the application of secure by design principles and a credible secure by design methodology that integrates security considerations into the design process and security measures into SSCs, in a way that is consistent with the operational intent of the RR SMR, and before the application of dedicated security controls.

This Level 1 Security sub-claim is supported by a set of underlying nuclear security specific sub-claims, as summarised in Table 32.14-1.

Table 32.14-1: Nuclear Security Sub-claims - Secure by Design

Security Sub-claims Level 2	**Security Sub-claims Level 3**
[32.1.1] Relevant analyses of security threat have been undertaken, and in accordance with the Secure by Design concept, where unacceptable risks have been identified design changes have been recommended.	[32.1.1.1] Security risk inherent in the design has been minimised through the application of a credible secure by design methodology that includes security design principles and integrates security analyses and design activities into the engineering process, such that security risk is eliminated or minimised before the application of security controls, in a way that is consistent with the operational intent of the RR SMR.
	[32.1.1.2] The capabilities of threat actors and the ways in which they might exploit the design to cause a radiological release, steal nuclear material or compromise sensitive nuclear information are understood, and the design incorporates integrated security measures to defend against these capabilities where this is practical and consistent with the operational intent of the RR SMR.
	[32.1.1.3] Provision has been made in the design to accommodate dedicated security measures required to achieve the necessary security Outcomes.
	[32.1.1.4] Where improvements to the methodology are identified during its application or analysis these are fed back to the methodology author.
[32.1.2] Potential options for plant layout have been identified and considered to eliminate or reduce associated nuclear security risk.	[32.1.2.1] An initial security assessment of the design has been undertaken to identify sources of security risk.
	[32.1.2.2] Design changes that eliminate or reduce sources of security risk inherent in the design have been recommended.
	[32.1.2.3] Recommended design changes have been screened for their impact to safety and operation of the RR SMR.
	[32.1.2.4] Acceptable design changes have been incorporated into the design.

Security Sub-claims Level 2	**Security Sub-claims Level 3**
[32.1.3] The capabilities and likely goals of threat actors are understood.	Not currently used
[32.1.4] A relevant security analysis of the design has been undertaken to identify the ways in which the design may be exploited to cause a radiological release, steal nuclear material or other radioactive material, or compromise sensitive nuclear information.	[32.1.4.1] The postulated scenarios have been screened to eliminate any scenarios for which threat actors do not possess the necessary capability.
	[32.1.4.2] Design changes that prevent the realisation of credible scenarios, or make their realisation more difficult, have been proposed.
	[32.1.4.3] Recommended design changes have been screened for their impact to safety and operation of the RR SMR.
	[32.1.4.4] Acceptable design changes have been incorporated into the design.
[32.1.5] Dedicated security measures required to achieve the necessary security Outcome have been proposed.	[32.1.1.1] Security risk inherent in the design has been minimised through the application of a credible secure by design methodology that includes security design principles and integrates security analyses and design activities into the engineering process, such that security risk is eliminated or minimised before the application of security controls, in a way that is consistent with the operational intent of the RR SMR.
	[32.1.1.2] The capabilities of threat actors and the ways in which they might exploit the design to cause a radiological release, steal nuclear material or compromise sensitive nuclear information are understood, and the design incorporates integrated security measures to defend against these capabilities where this is practical and consistent with the operational intent of the RR SMR.
	[32.1.1.3] Provision has been made in the design to accommodate dedicated security measures required to achieve the necessary security Outcomes.

32.15 Appendix B: Nuclear Security - to Categorisation for Theft

The Categorisation for Theft is the subject of a Level 1 security specific E3S sub-claim, as follows:

- [32.2] – The Nuclear Material (NM) & Other Radioactive Material (ORM) inventories have been categorised, using an appropriate Categorisation for Theft agreed methodology, for the purpose of identifying the level of protection from theft that is required.

This Level 1 Security Sub-claim is supported by a set of underlying nuclear security specific sub-claims, as summarised in Table 32.15-1.

Table 32.15-1: Nuclear Security Sub-Claims - Categorisation for Theft

Security Sub-claims Level 2	Security Sub-claims Level 3
[32.2.1] The Nuclear Material (NM) & Other Radioactive Material (ORM) inventories have been categorised, using an appropriate Categorisation for Theft agreed methodology, for the purpose of identifying the level of protection from theft that is required.	[32.2.1.1] – A suitable nuclear inventory, comprising Nuclear Material (NM) and Other Radioactive Material (ORM) has been established for the generic RR SMR.
	[32.2.1.2] - Targets and their locations requiring protection against theft have been identified and suitably categorised for security purposes.
[32.2.2] Following the Categorisation for Theft of the Nuclear Material (NM) & Other Radioactive Material (ORM) inventories, any applicable recommendations for risk reduction were proposed and reported to the relevant design team.	Not currently used
[32.2.3] The security requirements identified through Categorisation for Theft Methodology were developed further as part of an overall Integrated Security Solution for the generic RR SMR, which addresses physical, cyber and blended threats.	Not currently used

32.16 Appendix C: Nuclear Security Sub-claims - Cyber Security and Information Assurance

The Cyber Security & Information Assurance (CS&IA) is the subject of a Level 1 security specific E3S sub-claim, as follows:

- [32.3] Cyber Security & Information Assurance (CS&IA): The risks to all digital assets (including Operational Technology [OT] and Information Technology [IT]) associated with the generic RR SMR shall be reduced to an acceptable level through the use of CS&IA as part of a larger Cyber Protection System (CPS), within an Integrated Security Solution (ISS). Risks to be mitigated include sabotage resulting in an Unacceptable radiological Consequence, the theft of nuclear/radiological materials, the compromise of sensitive nuclear information, as well as lesser consequences such as plant interruptions, industrial hazards and lesser radiological consequences.

This Level 1 Security sub-claim is supported by a set of underlying nuclear security specific sub-claims, as summarised in Table 32.16-1: Nuclear Security Sub-claims - Cyber Security and Information Assurance .

Table 32.16-1: Nuclear Security Sub-claims - Cyber Security and Information Assurance

Security Sub-claims Level 2	Security Sub-claims Level 3
[32.3.1] Policies and procedures shall be put in place to manage cyber risk in accordance with recognised international standards and RGP, with defined roles and responsibilities, and communication routes.	Not currently used
[32.3.2] Cyber security risks shall be assessed using threat-based risk assessment process utilising the RR SMR Threat Interpretation to provide a graded security approach based on the system consequences.	Not currently used
[32.3.3] Cyber security control sets shall be implemented to reduce cyber security risks to an acceptable level, in a graded approach based on the consequences of system compromise and the skill of the threat actor.	[32.3.3.1] Cyber security risks to CBSIS and CBSy that could result in an Unacceptable Radiological Consequence shall be mitigated to an acceptable level.
	[32.3.3.2] Cyber security risks to CBSIS and CBSy that could result in the theft of nuclear material and other radiological material shall be mitigated to an acceptable level.
	[32.3.3.3] Cyber security risks associated with operational issues, industrial hazards and lesser radiological doses (below the level of an URC) shall be mitigated to an acceptable level.
[32.3.4] Sensitive Nuclear Information shall be subject to appropriate security controls to maintain its confidentiality, integrity and availability	[32.3.4.1] Cyber security risks associated with the compromise of SNI shall be mitigated to an acceptable level.
[32.3.5] Cyber security controls shall be implemented was part of an Integrated Security Solution (ISS) in conjunction with physical Regulatory Framework for the Nuclear Security Case	Not currently used

32.17 Appendix D: Nuclear Security Sub-claims - Vital Area Identification and Categorisation

VAI&C is the subject of a Level 1 security specific E3S sub-claim, as follows:

- [E3S Claim 32.4] Protection from Sabotage: The design basis threat of the sabotage of nuclear material or other radioactive material which could result in Unacceptable Radiological Consequence will be managed through the application of a Vital Area Identification and Categorisation (VAI&C) Methodology to identify requirements for proportionate security measures. These security measures will form part of an Integrated Security Solution (ISS) for the generic RR SMR.

This Level 1 Security sub-claim is supported by a set of underlying nuclear security specific sub-claims, as summarised in Table 32.17-1.

Table 32.17-1: Nuclear Security Sub-claims - Vital Area Identification and Categorisation

Security Sub-claims Level 2	Security Sub-claims Level 3
[32.4.1] A structured Vital Area Identification and Categorisation (VAI&C) methodology has been developed and applied in line with the relevant good practice (both international and UK national) for the identification of Vital Areas for the RR SMR. This methodology identifies potential physical and cyber threats which could result in an Unacceptable Radiological Consequence (URC).	[32.4.1.1] – The Vital Area Identification and Categorisation (VAI&C) methodology forms part of the overall Secure by Design approach adopted for the RR SMR, and through this is integrated with the relevant engineering processes.
	[32.4.1.2] – The Vital Area Identification and Categorisation (VAI&C) Methodology makes use of information from the other security analysis: • From the Categorisation for Theft methodology information regarding the nuclear inventory for a RR SMR • From the Cyber Security Risk Assessment (CSRA) methodology, the identification of Computer Based Systems important to Safety (CBSIS).
	[32.4.1.3] A nuclear inventory has been established for the generic RR SMR, comprising Nuclear Material (NM) and Other Radioactive Material (ORM). To allow the identification of Candidate Vital Areas, this inventory has been reviewed to establish those assets with the potential to give rise or contribute to an Unacceptable Radiological Consequences (URC) if sabotaged
	[32.4.1.4] Rolls-Royce SMR has identified Structures Systems and Components (SSCs) required to prevent, protect or mitigate against Initiating Events of Malicious Origin (IEMO), directed against Nuclear Material (NM) and Other Radioactive Material (ORM), progressing to Unacceptable Radiological Consequences (URC).
	[32.4.1.5] Rolls-Royce SMR has assessed the credibility of the applied design basis threat to result in a URC through sabotage of the Targets (NM/ORM and preventative/protective/mitigating SSCs) as a result of physical, cyber or blended attacks.
	[32.4.1.6] Vital Areas have been established based on the Targets (NM/ORM and preventative/protective/mitigating SSCs) requiring protection from sabotage and their locations.
[32.4.2] The vulnerability to sabotage of SSCs (as a result of a physical, cyber or blended attack) have been reduced through the application of Secure by Design. This has resulted in the	[32.4.2.1] Prior to the formal application of the VAI&C Methodology, the interaction of Security SMEs in the early stages of design processes, considered whether the sabotage of the SSCs concerned could contribute to an Unacceptable Radiological Consequence (URC)

Security Sub-claims Level 2	Security Sub-claims Level 3
minimisation of the scope and number of Vital Ares (and where practical) a reduction in the categorisation of such	and sought to influence design in order to reduce the risk. This includes influence on site layout and modularisation and the (Safety Case) requirements for segregation and diversity.
	[32.4.2.2] Where Candidate Vital Areas were identified, by the VAI&C Methodology, the causes for their identification were analysed, and where applicable recommendations for risk reduction were proposed and reported to the relevant design team. This is an iterative process, repeated at various stages during the design of the relevant SSCs.
	[32.4.2.3] Identified Vital Areas (remaining after design modifications) have been categorised based upon the consequences of the sabotage of such; this supports the development of proportional security measures.
[32.4.3] The security solutions to address the sabotage risk (from physical, cyber or blended attack) to the identified Vital Areas are developed and included with the Integrated Security Solution for the generic RR SMR.	Not currently used

32.18 Appendix E: Nuclear Security Sub-claims - Integrated Security Solution

The Integrated Security Solution is the subject of a Level 1 security specific E3S sub-claim, as follows:

- [E3S Claim 32.5] The Integrated Security Solution (ISS) has been developed for the generic RR SMR. The ISS provides future Operators with a full understanding of the security solution and how it has been developed; and provides the basis for the subsequent development of a security plan for an operational RR SMR which will both meet regulatory expectations for nuclear security and address the commercial risk appetite of the Operator.

This Level 1 Security sub-claim is supported by a set of underlying nuclear security specific sub-claims, as summarised in Table 32.18-1.

Note: Rolls-Royce SMR recognizes that this current roadmap for the ISS claims would benefit from some revision, addition and restructuring.

Table 32.18-1: Nuclear Security Sub-claims - Integrated Security Solution

Security Sub-claims Level 2	**Security Sub-claims Level 3**	**Security Sub-claims Level 4**
[32.5.1] The Integrated Security Solution (ISS) is based around security infrastructure which provides for both a Physical Protection System (PPS) and a Cyber Protection System (CPS). The framework for the development of the security infrastructure ensures that it is integrated into the plant design to provide a holistic security approach for the generic RR SMR.	[32.5.1.1] The framework for the development of the Integrated Security Solution is built upon current Relevant Good Practice (RGP); this includes guidance from the IAEA and more specific UK national guidance which include ONR Security assessment Principles (SyAPs) and Technical Assessment Guidance (TAGs), guidance from the National Protective Security Agency (NPSA), and other experience from nuclear and non-nuclear sectors.	[32.5.1.1.1] The framework for design of the Security Infrastructure is integrated into the Rolls-Royce SMR Secure by Design approach and through this into engineering design.
		[32.5.1.1.2] Security requirements have been taken into consideration in the design of the building layout, including the impact of modularisation.
		[32.5.1.1.3] Deconfliction with safety requirements, environmental control measures and outage/maintenance activities, has occurred as part of the integrated E3S design process.
	[32.5.1.2] The Physical Protection System (PPS), which is based on output of the relevant security analyses, protects against malicious events that could result in an Unacceptable Radiological Consequence (URC), the theft of Nuclear Material (NM) or Other Radioactive Material (ORM) and the compromise of Sensitive Nuclear Information (SNI).	[32.5.1.2.1] Defines the level of physical protection provided within the design, based on the output of Security Analyses (e.g. VAI&C, Theft and Vulnerability Assessment) against the Final Concept Design (FCD)

Security Sub-claims Level 2	Security Sub-claims Level 3	Security Sub-claims Level 4
		[32.5.1.2.2] Defines Physical Security Functions required to remove or mitigate the identified events of malicious origin.
		[32.5.1.2.3] Defines Physical Security Functions required to mitigate actions by threat actors, including Deter, Detect, Delay, Assess, Access Control, and Insider Threat Measures.
		[32.5.1.2.4] Identifies the Physical Security Measures selected to provide the appropriate level of physical response.
		[32.5.1.2.5] Demonstrates the concept selection and optioneering of the physical protection design solutions meet the desired outcome through the application of Vulnerability Assessments.
		[32.5.1.2.6] Demonstrates how power requirements for SSCs with security functions, and security systems, have been included within the building design.
		[32.5.1.2.7] Identifies those requirements and assumptions for the secure operation of the PPS, to ensure the desired outcomes are achieved. This includes, where temporary Vital Areas exist, their location, the time at risk and the measures necessary to ensure the security outcomes are met.

Security Sub-claims Level 2	Security Sub-claims Level 3	Security Sub-claims Level 4
		[32.5.1.2.8] Defence in Depth is achieved by establishing physical security zones, to limit access to sensitive areas or for the segregation and separation of safety systems.
		{32.5.1.2.9] Human Factors principles will be applied to the security measures to identify Human Based Security Claims with the PPS.
	[32.5.1.3] The Cyber Protection System (CPS); which is based on output of the relevant security analyses protects against malicious events that could result in an Unacceptable Radiological Consequence (URC), the theft of Nuclear Material (NM) or Other Radioactive Material (ORM) and the compromise of Sensitive Nuclear Information (SNI).	[32.5.1.3.1] Defines the level of cyber protection provided within the design, based on output of Security Analyses against FCD
		[32.5.1.3.2] Defines the Cyber Security Functions required to remove or mitigate the identified events of malicious origin.
		[32.5.1.3.3] Defines Cyber Security Functions required to mitigate actions by threat actors, including Identify, Protect, Detect, Respond and Recover.
		[32.5.1.3.4] Identifies the Cyber Security Measures selected to provide the appropriate level of response.

Security Sub-claims Level 2	**Security Sub-claims Level 3**	**Security Sub-claims Level 4**
		[32.5.1.3.5] Demonstrates the concept selection and optioneering of the cyber protection solutions meet the desired outcome through, repeated cycles of Cyber Security Risk.
		[32.5.1.3.6] Identifies those requirements and assumptions for the secure operation of the CPS, ensuring the desired outcomes are achieved.
		[32.5.1.3.7] Identifies those requirements and assumptions necessary for the secure operation of the site IT/OT network(s), including those for Emergency Planning, Exercising and Recovery.
		[32.5.1.3.8] Human Factors principles will be applied to the security measures to identify Human Based Security Claims with the CPS.
[32.5.2] The Integrated Security Solution (ISS) provides the basis for a security plan for an operational site, that is a Nuclear Site Security Plan (NSSP) for a UK deployed RR SMR or similar under other national regulatory regimes.	[32.5.2.1] The ISS provides a future Operator with a full understanding of the security solution for generic RR SMR and how it has been developed.	Not currently used
	[32.5.2.2] The ISS provides a definition of the Security Infrastructure (including that within engineering/civil/layout design) that contributes to the delivery of the security solution.	Not currently used

Security Sub-claims Level 2	Security Sub-claims Level 3	Security Sub-claims Level 4
	[32.5.2.3] The ISS considers all Operational states, including normal power production and routine outages.	Not currently used
	[32.5.2.4] The ISS considers all stage in the plants Lifecycle from initial fuelling, through normal operations and ultimately to de-fuelling and decommissioning.	Not currently used
	[32.5.2.5] The ISS sets out the assumptions regarding the operation of the security solution. The ISS will provide 'Security Tech Specs' around the security solution and allow the Operator to understand the impact of varying any of these 'Security Tech Specs.	[32.5.2.5.1] The ISS specifies site-specific 'Security Tech Specs' rules that must be adhered to, to ensure the security outcomes are met, including the logic used derive these rules.
		[32.5.2.5.2] The ISS allows the operator to trace 'Security Tech Specs' to the original design assumptions and requirements.
	[32.5.2.6] The ISS sets out and what the Operator owned risks that need addressing within the site-specific security plan.	[32.5.2.6.1] The ISS details any residual Regulatory Risk outstanding within the 'Detailed Generic Design'.
		[32.5.2.6.2] The ISS details assumptions made within the Generic Design that may necessitate for Site-Specific Design
		[32.5.2.6.3] The ISS details assumptions made within the design that include 'accepted' Commercial Risks and those where ongoing mitigation is required.

32.19 Appendix F: Integration between Nuclear Security and Other Topic Areas

Table 32.19-1: Integration between Nuclear Security and other E3S Topic Areas

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
Chapter 3: E3S Objectives & Design Rules for Structures, Systems & Components	Presents the key principles and associated methods, approaches, and requirements that provide the framework for the RR SMR to achieve its E3S objectives.	To capture security design requirements to be placed onto relevant Structures, Systems and Components (SSCs) and to integrate the Security Functional Categorisation and Classification of SSCs with those for Safety, Environment and Safeguards.
Chapter 4: Reactor (Fuel & Core)	Describes the fuel and core design, including its composition and configuration of fuel, control rods, etc., and associated operational parameters.	The system designs at the Final Concept Definition (FCD will be used to support the Vital Area Identification assessment).
Chapter 5: Reactor Coolant System & Associated Systems	Describes the Reactor Coolant System (RCS) and associated systems, which include the Reactor Pressure Vessel (RPV) and the primary coolant circuit components.	Candidate IEMOs and Candidate Sabotage Event Scenarios will be identified and taken through the Vital Area Identification and Categorisation Methodology (VAI&CM). Opportunities to design out security vulnerabilities by applying the Secure by Design principle will be passed to the system design engineers, and requirements to design in passive and active security measures will be passed to the layout engineers. Chapter 4 – Fuel & Core – will also inform the inventory of NM/ORM to categorise material for theft and be used in the VAI&CM.
Chapter 6: Engineered Safety Features	Describes the systems which deliver the safety functions in response to fault and accident conditions in the reactor.	

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
Chapter 7: Instrumentation & Control	Describes the Control & Instrumentation (C&I) systems of the RR SMR which support delivery of the safety functions.	The overall C&I architecture designs for the Reactor Protection System, Diverse Protection System Accident Management System, and Reactor Plant Control and Monitoring System are based on non-functional system requirements derived from United Kingdom and international Relevant Good Practice (RGP) and Operating Experience (OPEX). The application of the Cyber Security Risk Assessment Methodology to these C&I systems will identify opportunities to design out cyber security vulnerabilities (SbyD principle) and, where necessary, to identify control sets that should be designed in to protect the systems from relevant threats. These outputs will support the preliminary evidence available at the FCD design stage to underpin the high-level Claim that the RR SMR C&I is designed and substantiated to achieve functional and non-functional safety and security requirements through the lifecycle and reduce risks to ALARP.
Chapter 8: Electrical Power	Describes the electrical power systems which supply power to systems during both normal and fault conditions.	The high-level overview of the electrical sub-systems architecture and the functions they deliver will be assessed to determine whether they can be used to support the creation of Candidate IEMOs and Candidate Sabotage Event Scenarios via the VAI&CM.

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
Chapter 9A: Auxiliary Systems	Describes the auxiliary systems of the RR SMR, including the fresh fuel and spent fuel storage and handling systems, spent fuel cooling and clean-up systems, systems for transfer of new and spent fuel between fuel pools, refuelling systems, main cooling water system, component cooling system, essential service water system, and auxiliary cooling and make-up system.	The auxiliary systems will be assessed to determine whether they can be used to support the creation of Candidate IEMOs and Candidate Sabotage Event Scenarios via the VAI&CM. Opportunities to design out security vulnerabilities by applying the Secure by Design principle will be passed to the system design engineers, and requirements to design in passive and active security measures will be passed to the layout engineers. The Chapter will also inform the inventory of NM/ORM to categorise material for theft and be used in the VAI&CM.
Chapter 9B: Civil Engineering Works and Structures	Describes the civil and structural design aspects of the RR SMR, including the hazard shield and the base isolation system for protection against external hazards.	The civil and structural designs will be reviewed against the adversary capabilities described in the GSR Threat Interpretation document. Potential security vulnerabilities will be identified and presented to the structural engineers to design out, and the GSR will make claims against those structures that support the delivery of the security functions and will form part of the PPS.
Chapter 11: Management of Radioactive Waste	Describes the radioactive waste treatment systems for the RR SMR, and summarises the sources of solid, liquid, and gaseous waste streams as well as the anticipated quantities, arrangements for waste minimisation, and disposal routes.	Management of Radioactive Waste

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
Radiation Protection	Evaluates how radiation doses to onsite workers and members of the public will be controlled during normal operations and describes the design features of the RR SMR that minimise exposures to ALARP.	Knowledge of the locations, types and quantities of sources of ionising radiation at all plant states is essential to inform the inventory of NM/ORM to support the assessment of material against theft and sabotage. This includes contained, immobile and airborne sources. Awareness of the design features for radiation protection and radiation and contamination zoning inform the formation of Candidate Sabotage Event Scenarios, which will be used in the VAI&CM. The GSR will also consider taking credit for any protection features that may protect the material from theft or sabotage. The Secure by Design principle will be employed to design out any security vulnerabilities, which could include measures already identified to minimise the source term.
Chapter 13: Conduct of Operations	Presents how the RR SMR fulfils its prime responsibility for the safety in operation, including organisational arrangements, competencies and training programmes, operational safety programmes, and operating procedures and guidelines.	The Chapter will be reviewed against the ISS to confirm that the philosophies and procedures within the safety and security aspects of the E3S Case complement each other where applicable, and that points of conflict are identified and resolved. The GSR will link into Section 13.2 – Nuclear Safety and Security Interfaces – of the Chapter.
Chapter 15: Safety Analysis	Presents the methods and outputs of the safety analysis that evaluate the RR SMR against relevant criteria and	The outputs from the Safety Analysis will be key inputs to develop Candidate IEMOs and Candidate Sabotage

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
	inform the design development, including the deterministic analysis of faults and accidents, probabilistic analysis, and internal and external hazard assessment.	Event Scenarios via VAI&C and subsequent assessments. Direct inputs will be fed from the development of the Fault Schedule and fault sequences for each Postulated Initiating Event identified.
Chapter 16: Operational Limits & Conditions	Presents the processes to define the Operational Limits & Conditions (OLCs) in the design and safety analysis, to ensure they are successfully transferred into operational documentation.	An understanding of the E3S design principles and requirements, and their flow into Operations to maintain OLCs, will be used in the GSR to create Candidate IEMOs and Candidate Sabotage Event Scenarios in the VAI&CM and subsequent assessments.
Chapter 18: Human Factors Engineering	Provides the demonstration that Human Factors (HF) is fully integrated into the RR SMR design and substantiation processes.	Assessment of Human Reliability Analysis has identified potential Human Based Safety Claims (HBSC) – where human actions are claimed to prevent, recover or mitigate against faults – which will reviewed as potential causes of Candidate IEMOs and Candidate Sabotage Event Scenarios in the VAI&CM and subsequent assessments. Similarly, Human Failure Events, which are negative descriptors of HBSCs, will input into the VAI&CM and assessments.
Chapter 22: Conventional & Fire Safety	Presents the strategies for implementation of conventional and fire safety into design of the RR SMR, including Construction Design and Management.	The design of integrated PPS and CPS within the ISS might introduce security measures that contradict the design requirements for conventional and fire safety solutions. This will involve emergency evacuation routes and ingress points for emergency responders.

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
		The outputs from this Chapter will be reviewed against the integrated security solutions in the ISS Report.
Chapter 23: Structural Integrity	Presents the RR SMR demonstration of structural integrity for safety-classified metallic pressure boundary components and their supports.	The structural integrity of SSCs and their substantiation will be inputs into the VAI&CM and assessments for theft and sabotage. The Secure by Design principle will be applied, and the outputs will be passed back to the relevant designers.
Chapter 25: Detailed information about the design	Presents a technical description of the facility's main plants, systems and processes, which have a bearing on radioactive waste (solid, liquid and gaseous) generation, treatment, measurement, assessment and disposal, drawing upon information from other E3S Case chapters.	The outputs from this Chapter will inform the Plant and Design Information report and input into the VAI&CM and assessments for theft and sabotage.
Chapter 26: Detailed description of radioactive waste management arrangements	Presents the Radioactive Waste Management Arrangements (RWMA) for RR SMR, including an overview of waste minimisation with focus on disposability and optimised disposal routes.	The waste strategies and management plans will input into the inventory of NM/ORM and inform the categorisation for theft and sabotage. Account will be taken of the potential fluctuation in waste quantities. The locations, quantities and transfer methods of wastes must demonstrate BAT, which includes considerations from the Security Case. Therefore, the Secure by Design principle will be applied, and the outputs will be passed

E3S Chapter	Outline Scope of Topic Area	Interaction with GSR
		back to the relevant designers.
Chapter 33: Safeguards	Presents the demonstration that the design of RR SMR facilitates Safeguards through material accountability, and containment and surveillance	Safeguards measures will need to be built into the designs of facilities and SSCs to prevent the diversion of Qualifying Nuclear Materials. There are likely to be overlaps between Safeguards and Security requirements and these will be inputs into the ISS Report.

32.20 Glossary of Terms and Abbreviations

ALARP	As Low As Reasonably Practicable
BAT	Best Available Techniques
BEIS	(former) Department for Business, Energy & Industrial Strategy
CAE	Claims - Argument - Evidence
CAPSS	Cyber Assurance of Physical Security Solutions
CBSESO	Computer Based Systems Essential to Safe Operations
CBSIS	Computer Based Systems Important to Safety
CBSy	Computer Based Security
CCTV	Closed Circuit Television
CfT	Categorisation for Theft
C&I	Control and Instrumentation
CNI	Critical National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CSRA	Cyber Security Risk Assessment
CS&IA	Cyber Security and Information Assurance
CPS	Cyber Protection System
CSRAM	Cyber Security Risk Assessment Methodology
CSSP	Construction Site Security Plan
DOORS	Dynamic Object-Orientated Requirements System
DPS	Diverse Protection System
DR	Definition Review
DRP	Design Reference Point
ECC	Emergency Control Centre
E3S	Environment, Safety, Security and Safeguard
EP&R	Emergency Planning and Response
ERC	Emergency Response Centre

ESSSESP	Engineer Safe, Secure, Safeguarded and Environmentally Sound Products
FCD	Final Concept Definition
FMEA	Failure Modes and Effects Analysis
FSF	Fundamental Safety Function
FSyP	(ONR) Fundamental Security Principle
GDA	Generic Design Assessment
GSR	Generic Security Report
HCVA	High Consequence Vital Area
HF	Human Factors
HMV	Hostile Vehicle Mitigation
IAEA	International Atomic Energy Agency
ICSANT	International Convention for the Suppression of Acts of Nuclear Terrorism
IE	Initiating Event
IEMO	Initiating Event of Malicious Origin
IMS	Integrated Management System
ISS	Integrated Security Solution
ILW	Intermediate Level Waste
IT	Information Technology
KSyPP	(ONR) Ket Security Plan Principle
LLW	Low Level Waste
MCR	Main Control Room
NISR 2003	Nuclear Industries Security Regulations 2003
NIST	National Institute for Science and Technology

NSL	Nuclear Site Licence
NM	Nuclear Material
NPP	Nuclear Power Plant
NPSA	National Protective Security Authority
NSSP	Nuclear Site Security plan
OLC	Operating Limits and Conditions
ONR	Office for Nuclear Regulation
ONRCNSS	Office for Nuclear Regulation Civil Nuclear Security and Safeguards
ORM	Other Radioactive Material
OT	Operational Technology
PAA	Preliminary Assumption-based Assessment
PCD	Preliminary Concept Definition
PSES	Potential Sabotage Event Scenarios
PPS	Physical Protections System
RASyP	(ONR) Regulatory Assessment of Security Plans
RD	Reference Design
RDS-PP	Reference Designation System for Power Plants
RGP	Relevant Good Practice
RR SMR	Rolls-Royce Small Modular Reactor
RPS	Reactor Protection System
RWMA	Radioactive Waste Management Arrangements
SAPs	(ONR) Safety Assessment Principles
SbyD	Secure by Design
SCP	Security Contingency Plan
SCR	Supplementary Control Room
SES	Sabotage Event Scenarios
SLC	Site Licence Condition
SME	Subject Matter Expert
SOCPA 2005	Serious Organised Crime and Police Act 2005

SSC	Structure, System, Component
SOPR	Security Outcomes Postures and Responses
SSyP	SMR Security Principle
SyAPs	Security Assessment Principles
SyCC	Security Control Centre
SyDP	(ONR) Security Delivery Principles
TAG	(ONR) Technical Assessment Guide
URC	Unacceptable Radiological Consequence
VA	Vital Area
VAI&C	Vital Area Identification and Categorisation