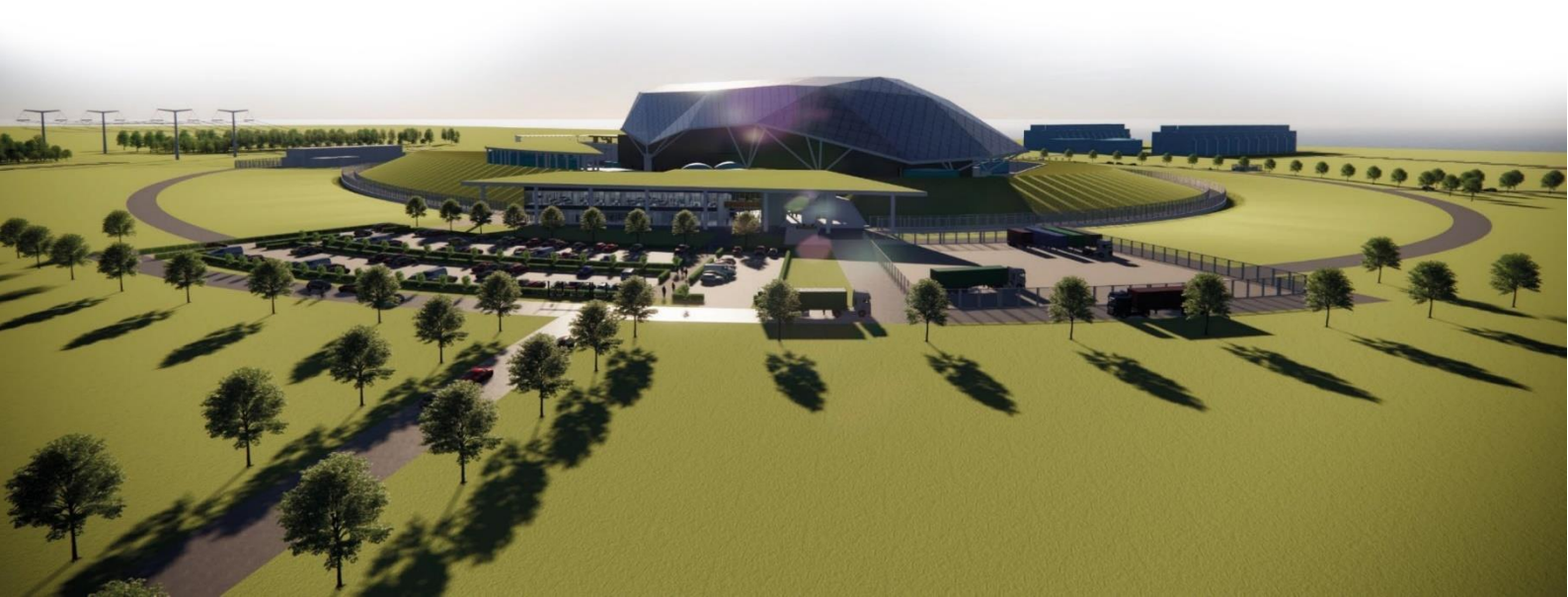
Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 32: Generic Security Report



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
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) • Confirmation 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 (section 32.7.8) • 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) Minor template/editorial updates for clarification and overall E3S Case consistency
August 2025	4	Issue	Version 3 of the Chapter supports and incorporates Design Reference Point 4. Changes include: • Updated claims structure (section 32.1.3 and Appendices)

Date	Revision Number	Status	Reason for Change
			• Examples of influence of Secure by Design on RR SMR engineering design (Table 32.4-1) • Summary Categorisation for Theft based on current knowledge of inventory (section 32.5.5) • Update of Cyber Security Risk Assessment (CSRA) methodology (sections 32.6.5 and 32.6.6) • Summary of CSRA for RPS DPS, RCPS PPCS (section 32.7.8) • Greater clarify around the approach to Vital Area Identification and Categorisation (VAI&C) (section 32.8.5) • Use of Preliminary Assumption-based Assessment (PAA) as precursor to VA&C (section 32.8.6.1) • Summary of findings for VAI&C for; reactivity control systems, reactor coolant systems, steam and feed systems ad containment systems (section 32.7.7) • Further detail on the approach to the development of the Integrated Security system (ISS), including initial concepts and a narrative of how the ISS develops over 2025 and 2026 (section 32.8)

Executive Summary

Chapter 32 of the E3S Case presents the Generic Security Report for the Rolls-Royce Limited Small Modular Reactor (RR SMR). The Chapter summarises the Security Case for the RR SMR as part of an integrated Environment, Safety, Security and Safeguards (E3S) Case for the RR SMR. Version 3 of the generic E3S Case is developed in support of the Design Reference Point 4 (DRP4).

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. SbyD links the identification of security risk to the development of the Integrated Security Solution (ISS) and links the development of the Security Case with both engineering design and the wider E3S Case. The ISS combines both a Physical Protection System (PPS) and Cyber Protection System (CPS).

This approach results in a design that:

- Protects against theft of nuclear material and the compromise of Sensitive Nuclear Information (SNI).
- Protects against cyber attacks which could compromise the safe operation of the RR SMR.
- Protects nuclear material and associated safety systems against sabotage (from both physical and cyber threats).

Overall, the Security Case contributes to an overall E3S case that demonstrates the RR SMR can be shutdown and brought to a safe state following an emergency incident.

The ISS protects the RR SMR through a combination of measures which deliver the following security functions:

- For the PPS – Deter, Detect, Delay, Assess, Control of Access, and Minimise Insider Threat.
- For the CPS - Identify, Protect, Detect, Respond and Recover.

The ISS provides a future Dutyholder / Licensee / 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, a future Dutyholder / Licensee / Permit Holder will be able to develop a security plan for an operational RR SMR.

Further submissions of the generic E3S Case are planned. Version 4 will be the last substantial revision of the case for GDA, and Version 5 will be a minor update to close-out any outstanding regulatory queries, observations and issues.

Contents

Tables

Figures

32.0 Introduction to Chapter

32.0.1 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.

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 3, Tier 1, Chapter 1: Introduction [1].

The generic E3S Case objective at Version 3 is

- Version 3 of the E3S Case shall provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective 'to protect people and environment from harm' as it is developed through detailed design. The Case shall demonstrate that risks are capable of being reduced to As Low As Reasonably Practicable (ALARP), using Best Available Techniques (BAT), will be secure/safeguarded by design, and demonstrate sustainability for current and future generations.

32.0.2 Objective and Scope of the Chapter 32

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 Security Case.

This version of Chapter 32 summarises the current development of the Security Case, with reference to other supporting documents or other sources of information. An indication is also given of the contents of future versions.

This chapter provides a proportionate summary of the arguments and evidence from lower tier information to underpin these. It draws upon information in relevant Tier 2 and Tier 3 documentation which forms part of the Nuclear Security Case as presented in the E3S Case Route Map [2].

This security specific Tier 2 and Tier 3 information references out (as relevant) to engineering design and layout information such as (but not limited to) system requirements specifications, system/safety measure design descriptions, layout summary reports, design decision records, and verification strategies.

The Security Case supports the development of a Nuclear Site Security Plan (NSSP) by a future Nuclear Site Licence (NSL) holder in the United Kingdom (UK). Key in achieving this objective is the Integrated Security Solution (ISS) for the RR SMR.

32.0.3 Claims, Arguments and Evidence Route Map

The E3S Case employs a Claims, Arguments, Evidence (CAE) framework to provide a structured demonstration that the RR SMR achieves the E3S fundamental objective 'to protect people and the environment from harm' through compliance with the E3S design principles, as described in E3S Case Version 3 Chapter 1: Introduction [1]. The CAE framework is presented in the E3S Case Route Map [2].

The claims decomposition for Chapter 32 is developed from the Fundamental E3S Objective [1] through the Fundamental Nuclear Security Claim, which is:

[Claim 32.0] The design of the RR SMR protects 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 Fundamental Security Claim is decomposed into a set of five high-level (Level 1) sub-claim s(see Sub-section 32.1.3.2)., which reflect the primary focus of a security regime to satisfy regulatory obligations (as outlined in the ONR SyAPs [15].

In accordance with the overall E3S Case, the Security Case is hierarchical in structural, comprising of three tiers (Tier 1, Tier 2 and Tier 3) of documentation.

Aspects of the CAE for Chapter 32 are further evidenced across other E3S Case chapters, including:

- Claims to justify that the security case meets the objectives and design rules for the RR SMR that are set out in E3S Case Version 3, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSC [3].
- Claims to justify that the Control & Instrumentation (C&I) and electrical systems deliver security functions are covered in E3S Case Version 3, Tier 1, Chapter 7: Control & Instrumentation [4] and E3S Case Version 3, Tier 1, Chapter 8: Electrical Power [5] respectively.
- Claims to justify that civil engineering and layout design are delivering security functions and contribution to the security solution for the RR SMR are covered in E3S Case Version 3, Tier 1, Chapter 9B, Civil Works and Structures [6].
- Claims to justify the allocation of operator actions to deliver security, and their substantiation, are covered in E3S Case Version 3, Tier 1, Chapter 18: Human Factors Engineering [7].
- Claims to justify the structural integrity of security classified Structures, Systems and Components (SSC) are covered in E3S Case Version 3, Tier 1, Chapter 23: Structural Integrity [8].

In addition to the claims addressed in this Chapter 32 with regard to SbyD, claims that holistically the plant can reduce risks to ALARP, demonstrate BAT, and ensure safeguards by design are underpinned in the relevant E3S Case Chapters.

Given the evolving nature of the generic E3S Case alongside the maturing design, some of the underpinning arguments and evidence remain under development. The conclusions of the chapter therefore provide an evaluation of how the arguments and evidence presented, and their trajectory, provide confidence in the case achieving its objective at this stage.

32.0.4 Context of the Security Case

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.

Monitoring and control of the RR SMR is centralised within the Main Control Room (MCR), located within the Reactor Island. A Security Control Centre (SyCC) provides a central point for the implementation and management of the security regime. 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.

The relative locations of the Reactor Island and Turbine Island (together with other selected SSCs) at Design Reference Point 4 (DRP4) are illustrated in Figure 32.0-1. Current design maturity includes for a separate 'off-site' Cooling Water Island. Further references to general arrangement drawings for the site are included in [1].

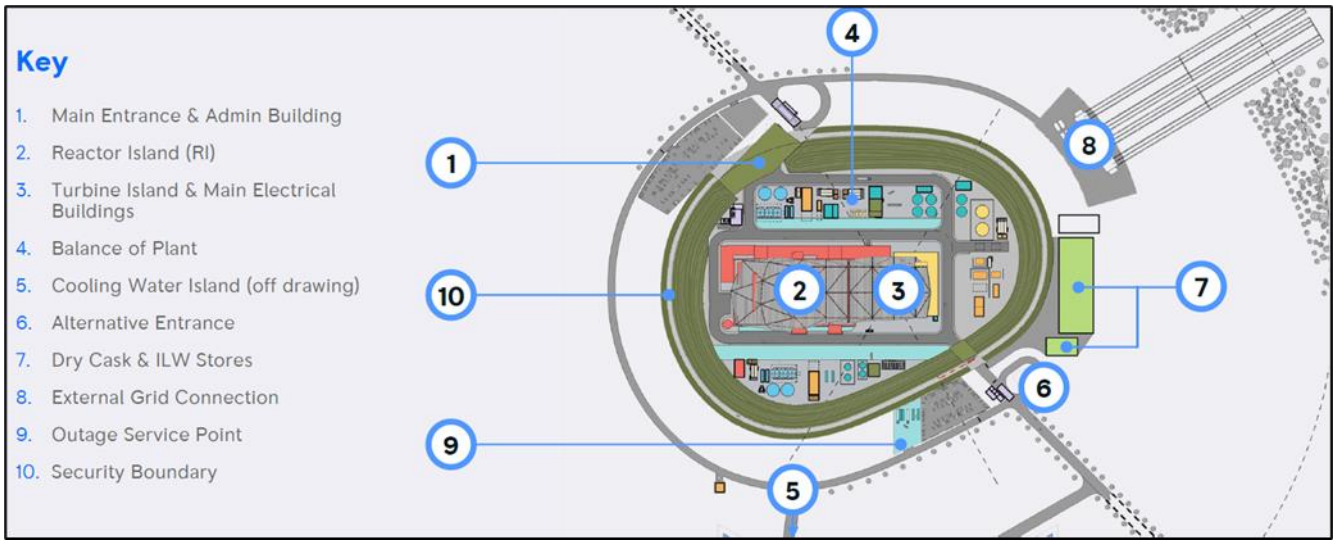


Figure 32.0-1: Indicative RR SMR Site Layout

A detailed summary of design and the engineering framework is provided in of the E3S Case, Version 3, Tier 1, Chapter 1: Introduction [1]. The design is 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 [9].

The Reactor Island houses many of the targets for sabotage and/or theft; and, therefore, provides a focus around which the ISS is 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. Dry Cask and Intermediate Level Waste (ILW) stores are not expected to be categorised as Vital Areas and so are shown outside the main security perimeter. However, security arrangements will still be considered from a commercial and Relevant Good Practice (RGP) perspective.

Relevant design information is also summarised in Tier 2 and Tier 3 of the Security Case, together with further reference to detailed engineering information. The security solution takes account of all operational states (see Section 1.8 of E3S Case Version 3, Tier 1, Chapter 1: Introduction [1].

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. Security Objectives are defined (see Sub-section 32.2.2.) and achieved through application of SbyD Principles (see Sub-section 32.2.3). This approach links the identification of security risk to the development of the Integrated Security Solution (ISS) and links the development of the Security Case with both engineering design and the wider E3S Case.

The ISS (see Section 32.8) combines both a Physical Protection System (PPS) and Cyber Protection System (CPS) which meet regulatory requirements through the delivery of security functions (see Sub-section 32.2.4).

A key criterion for the development of the ISS has been the compact and modular design of the RR SMR. This challenges the traditional approaches to nuclear security, which typically rely on a succession of barriers (and the distance between them) and other large structures to provide the opportunity to detect, delay and respond to adversaries.

32.0.5 Basis of the Security Case

Chapter 32 summarises the 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 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.

The Fundamental Nuclear Security Claim is decomposed into set of sub-claims (see Section 32.1) based on the five themes around which the Security Case is structured:

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

The nuclear security claim structure demonstrates how the security objectives for RR SMR (see Section 32.2.2) are met through the identification of security risk and as such how it will be protected against by an Integrated Security Solution ISS which comprises a combination of security measures integrated into engineering design and through dedicated security measures to address the residual risk. This is the SbyD approach (see Section 32.4).

The security analyses which identify the risks are undertaken against the UK national Design Basis Threat (DBT), which has been screened (to identify those threats which are specific to the RR SMR (see Section 32.3).

The threat profiles used in the analyses include for both physical and cyber threat scenarios and a blended attack (which combines both). The credibility of these scenarios is examined in the analysis with regard both to the capability of the attacker and the protection provided by the engineering design of the RR SMR and it component SSCs.

The security analyses include consideration of the potential for a sabotage attack which could compromise one or more of the Fundamental Safety Functions (FSFs); leading, if unmitigated, to a radiological release resulting in a dose at the site boundary sufficient for an Unacceptable Radiological Consequence (URC) to occur (see Sub-section 32.7.4).

The outputs from the security analysis (which are iterative in nature) are requirements on engineering design and site layout (to reduce risk) and/or requirements for dedicated security measures to address the residual risk. These requirements are for security measures which deliver both physical security functions and cyber security functions (see Sub-section 32.2.4). Security requirements are captured within the Rolls-Royce SMR Limited requirements management database [10].

The ISS protects Nuclear Material (NM) and Other Radioactive Material (ORM), safety critical SSCs and Sensitive Nuclear Information (SNI) against theft and sabotage; and RR SMR as a whole.

This protection is delivered through a combination of security measures which deliver the required security function in accordance with the Secure by Design principles (see Sub-section 32.2.3, including Defence in Depth (DiD) and the Graded Approach. This includes the protection of vital areas and other locations containing assets requiring protection (Graded Approach).

Features of the PPS include (see Sub-Section 32.8.6.3):

- The physical design and layout of the RR SMR delays the progress of any intruders through the site by means of security barriers, allowing time for a guard force to respond.
- Alarms and a CCTV system provide means of detection of unauthorised access to the site or parts of the site, and situational awareness of potential threat actors.
- Features such as exterior fences, CCTV, the berm, hostile vehicle mitigation and the presence of a guard force provide a visible deterrence.

Features of the CPS include (see Sub-section 32.8.6.4):

- Computer-based systems are assigned a security degree and a graded set of baseline security requirements, which are designed to reduce the risk of low-medium skill attackers.
- The Cyber Security Risk Assessment methodology identifies further system specific requirements that will account for higher skill adversaries.
- The architecture of the C&I segregates the control systems into zones and conduits – this defence in depth approach will delay attackers and limit propagation of malware.
- The Intrusion Detection System (Cyber) and logging and monitoring systems are designed such that unusual patterns in network traffic or user behaviour can be detected and investigated enabling timely response to events.

Both the PPS and CPS are designed with redundant and diverse measures (Defence-in-Depth) which seek to deter, detect and delay an attack and allow time for a response force to action.

The space and support systems necessary for the operation of the ISS security system are allowed for in the layout and design [6], including the provision of electrical power [5].

Facilities and space for an armed response force are included in the site design and layout, including allowance for defensive positions against an attack.

32.0.6 Structure of this Chapter

- Section 32.1, Introduction – This section discusses the purpose and introduces the contents of the document.
- Section 32.2, Security Case – This section introduces the scope of the 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 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 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.

32.0.7 Working Assumptions

The E3S Case is being developed alongside a maturing engineering design. In order to progress the E3S Case, it is necessary to make reasoned assumptions when design information is not yet available. As additional information becomes available, the validity of the assumptions is confirmed or otherwise.

For the purposes of the Security Case, assumptions are made to allow security analyses and the development of the ISS to proceed. These assumptions are collated in a Risks, Assumptions, Issues, Dependencies and Opportunities (RAIDO) Log [11]. The RAIDO Log has been created to document and track risks, assumptions, issues, dependencies, and opportunities identified during both formal security analyses, reviews, and informal engagements with engineering.

Working assumptions which are not validated will be passed on to be addressed by a future Dutyholder / Licensee / Permit Holder (see Sub-Section 32.0.8).

32.0.8 Assumptions and Commitments

An essential element of the generic E3S Case development process is the capture and tracking of assumptions and commitments that need to be passed on to a future Dutyholder / Licensee / Permit Holder at site-specific stage [12]. They are defined as:

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

The assumptions and commitments are captured within each chapter of the E3S Case and collated in Table 32.11-1 .

All E3S assumptions and commitments are logged in a case-wide 'Assumptions and Commitments for future Dutyholder / Licensee / Permit Holder Register' [13].

32.0.9 Limitations and Exclusions

32.0.9.1 Limitations

This issue of the Chapter 32 reflects the Security Case information available at the time of publication. The Security Case continues to mature, and future iterations will capture changes.

The current scope of the Security Case primarily addresses the operating phase of a nuclear power station. Security during manufacture, construction, or commissioning lifecycle phases will be covered in future iterations as the Security Case further develops.

Version 3 sets out the development of the security arrangements necessary to protect a single operational RR SMR unit. The possible implication of sharing security arrangements across co-located multiple units or across a fleet of locations will be considered, as necessary, in future site-specific security cases.

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, Version 3 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.

32.0.9.2 Exclusions

Chapter 32 does not cover the topic of Nuclear Safeguards. Nuclear Safeguards is covered within E3S Case Version 3, Tier 1, Chapter 33: Safeguards [14].

Version 3 does not consider the topic of security during the off-site transport of regulated nuclear material. This is a topic which is outside the scope of the security assessment at GDA.

32.0.10 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 [15].

32.1 Nuclear Security Case

32.1.1 Introduction

As noted in Section 0, the part of the E3S Case covering nuclear security, is referred to in this Chapter 32 as the Security Case.

The Security Case is presented as a hierarchy of documents that describe the conceptual security design, underpinned by risk-based analysis drawn from RGP. The security case summarises the NM, ORM, 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 Security Case presents evidence that the proposed design is likely to comply with Nuclear Industries Security Regulations 2003 (NISR 2003) [16]. It also demonstrates that regulatory expectations within the ONR Security Assessment Principles (SyAPs) [17] can be met.

32.1.2 E3S Case

Full details of the development, aims and scope of the E3S Case are included as E3S Case Version 3, Tier 1, Chapter 1: Introduction [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 [18]. The development of the generic E3S Case is, 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.

32.1.3 Security Case

As part of the overall E3S Case, the Security Case is developed to comply with relevant UK regulation and guidance (see Sub-section 32.1.5). 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 0, the E3S Case is using a CAE and presented in a tiered structure; this also applies to the 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.

32.1.3.1 Fundamental Nuclear Security Claim

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

[Claim 32.0] Fundamental Nuclear Security Claim: The design of the RR SMR protects 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 RGP, for example that promoted by the International Atomic Energy Agency (IAEA); and will be compliant with the relevant national regulatory regime.

The RR SMR nuclear security objectives (see Sub-section 32.2.2) reflect both: the moral obligation to protect people and the environment from harm (both conventional and nuclear) and that there are commercial imperatives on the security of the RR SMR which are drivers of engineering 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 (see Sub-section 32.2.3).

32.1.3.2 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 [17].

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

[Claim 32.1] 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.

Evidence and argument to underpin this claim is summarised in Section 32.4.

[Claim 32.2] Material at risk of theft is identified. Security measures are identified, and applied in a Graded Approach, to minimise the risk of theft.

Evidence and argument to underpin this claim is summarised in Section 32.5, which summarises the scope a SbyD Framework and how it is being applied to engineering design and layout to address vulnerabilities and reduce security risk.

[1] This excludes Scotland and Northern Ireland.

[Claim 32.3] Effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology (including Information Technology (IT) and Operational Technology (OT)) have been implemented and maintained.

Evidence and argument to underpin this claim is summarised in Section 32.6, which summarises a cyber security risk assessment process and it application to build in security controls into computer based systems and the CPS (as part of the overall ISS).

[Claim 32.4] The threat of sabotage of the Rolls-Royce SMR is minimised through the development of proportionate security measures as part of a Physical Protection System (PPS) which is included within an Integrated Security Solution (ISS).

Evidence and argument to underpin this claim is summarised in Section 32.7, which summarises a methodology for the identification and categorisation of sabotage risk. This in turn leads to recommendation for design in order to reduce security vulnerabilities. Protection requirements are identified for the PPS (as a part of an overall ISS).

[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.

Evidence and argument to underpin this claim is summarised in Section 32.8, which outlines the conceptual basis for the ISS and development of an integrated PPS and CPS which protection in line with required regulatory outcomes.

32.1.3.3 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:

- [Claim 32.1] - Secure by Design (in Appendix A in Section 32.13).
- [Claim 32.2] – Categorisation for Theft (in Appendix B in Section 32.15).
- [Claim 32.3] - Cyber Security & Information Assurance (in Appendix C in Section 32.15).
- [Claim 32.4] – Vital Area Identification and Categorisation (in Appendix D in Section 32.16).
- [Claim 32.5] - Integrated Security Solution (in Appendix E in Section 32.17).

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

As the overall E3S Case matures, relevant security case claims are aligned with relevant claims for other disciplines, for example claims made for layout and C&I design. This will be demonstrated further in future versions of the E3S Case.

32.1.4 Structure of Security Case

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

This Tier 1 chapter 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. These topic reports are

- Rolls-Royce SMR: Secure by Design Report [19].
- Rolls-Royce SMR Theft of Material and Categorisation for Theft Report [20].
- Rolls-Royce SMR Cyber Security Report [21].
- Rolls-Royce SMR Vital Area Identification and Categorisation Report [22].
- Rolls-Royce SMR: Integrated Security Solution [23].

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 supporting 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.

32.1.5 Regulatory Framework for the Security Case

32.1.5.1 Introduction

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

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

32.1.5.2 International Regulation and Guidance

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

- The Convention on the Physical Protection of Nuclear Material (CPPNM) - The CPPNM [24] 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) [25] 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 [26].
- Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), Implementing Guide No. 27-G, 2018 [27].

- Identification and Categorisation of Sabotage Targets and Identification of Vital Areas at Nuclear Facilities Nuclear Security Series No 48-T, 2024 [28].

32.1.5.3 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) [16] 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 the 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.

The ONR guidance includes that set out in the overarching ONR SyAPs [17] and supporting Technical Assessment Guides (TAGs).

32.1.5.4 ONR Security Assessment Principles

The primary purpose of the SyAPs [17] 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 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) [29].

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 (that is 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 (that is 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 not 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 the Security Case.

The SyAPs are accompanied by a series of Annexes [30] 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.

32.1.5.5 ONR Technical Assessment Guides (TAGs)

The ONR 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 [31].
- CNS-TAST-GD-6.2, Categorisation for Sabotage [32].
- CNS-TAST-GD-7.1, Effective Cyber and Information Risk Management [33].
- CNS-TAST-GD-11.4.1, Secure by Design [34].
- CNS-TAST-GD-11.4.2, The Threat [35].
- CNS-TAST-GD-11.4.5, Functional Categorisation and Classification of Security Structures, Systems and Components [36].

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.

32.2 Security Objectives and Principles

32.2.1 Introduction

32.2.1.1 Background

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.

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.

32.2.1.2 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.

32.2.1.3 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.

32.2.1.4 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 driven by consequence 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.

32.2.2 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.

32.2.3 Secure by Design Principles

The Rolls-Royce SMR Limited has defined a series of E3S Fundamental Principles [37]. 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 [37] and consistent with the expectations of the ONR SyAPs [17].

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 32.2-1).
- 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.

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.

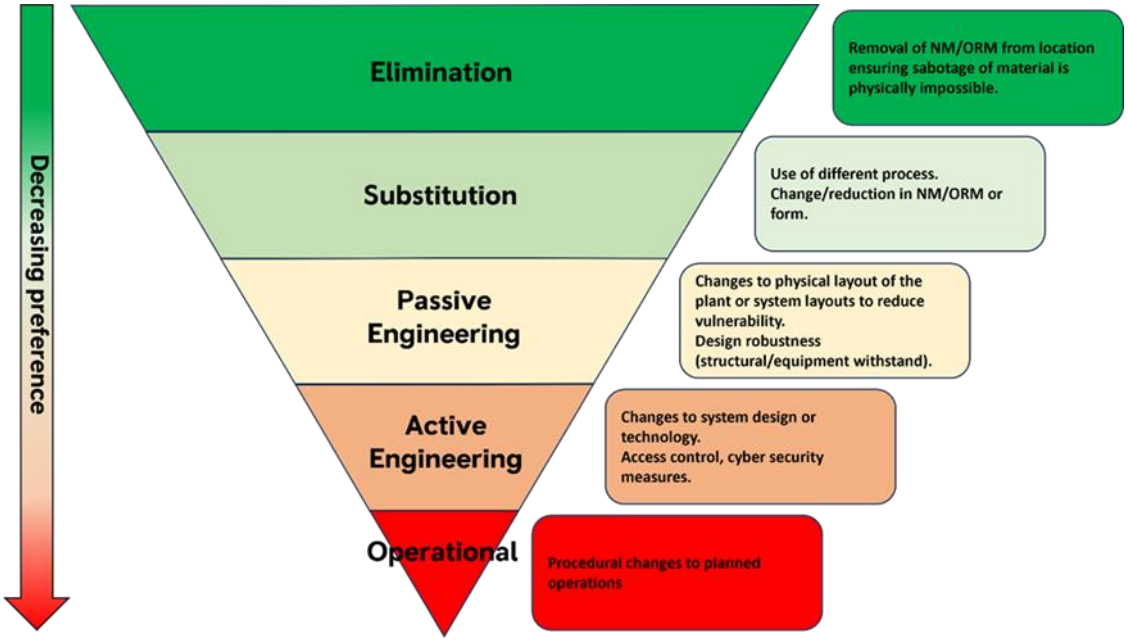


Figure 32.2-1: Hierarchy of Security Controls

32.2.4 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.
- Detect – systems and arrangements to alert a responding force to a potentially malicious or unauthorised act.
- Delay – provide a sufficiently robust design to permit a responding force to achieve the required outcome.
- 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 these security functions are illustrated on Figure 32.2-2. In practice, a combination of security function types is needed to achieve defence in depth.

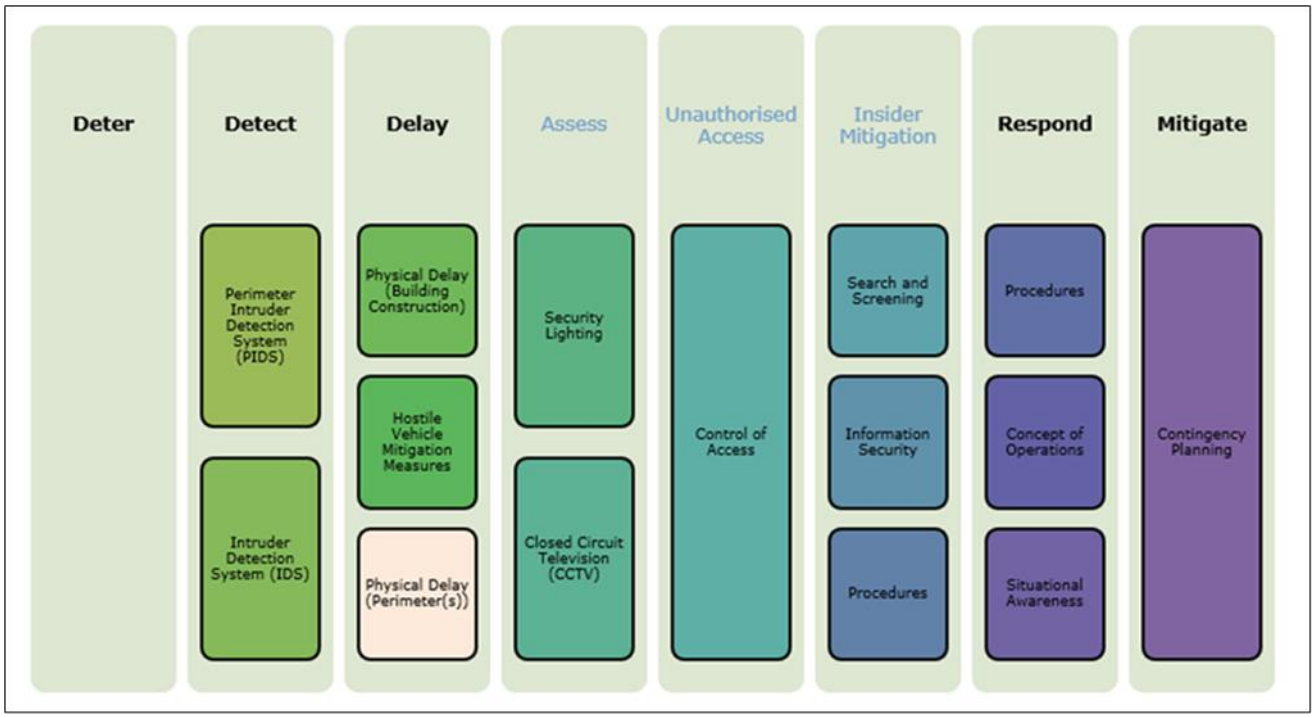


Figure 32.2-2: Layered Arrangements of Security Functions

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.

32.2.5 Integration of Nuclear Security into the RR SMR Design

32.2.5.1 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 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 32.2.3) and the interpretation of the UK 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 [10], 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.

Further detail on the interfaces between SbyD and the engineering design are found in the Tier 2 SbyD methodology [38].

32.2.5.2 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 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 given normally 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 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 Design Basis Threat (DBT). Hence, for the purposes of the security analysis, a conservative approach is adopted; whereby it is assumed generally 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 (at Version 3 of the E3S Case) of the probability of such an IEMO occurring or of the relative attractiveness of targets.

32.3 Threat Interpretation

32.3.1 Introduction

32.3.1.1 Introduction

The threat to be applied to the Security Case is mostly defined by the UK Government in the UK 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 [32].

Threat intelligence comes in a variety of forms. For physical and personnel security, this includes from the National Protective Security Authority quarterly briefings [39]. 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 [40], based upon the UK DBT, guidance from the ONR and other Government agencies. This Threat Interpretation is used as the basis for all current security assessment and has been produced to enable the consideration of threats from the DBT and elsewhere, i.e. from the DBT and beyond. This document is renewed as threat intelligence from government or other sources evolves.

32.3.1.2 Relevant Tier 2 and Tier 3 Evidence

This section of the Chapter 32 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 [40].

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

32.3.2 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 protects 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 Level 1 sub-claim is met.

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

32.3.3 Overview of Threat Interpretation

32.3.3.1 Threat Assessment

For this generic Security Case, the starting point for the threat assessment is the threats and capabilities outlined in the UK DBT, supplemented by additional information from relevant sources. 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.

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.

32.3.3.2 Target Identification

In determining the appropriate security measures for a PPS and a 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 [30].

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 [30]. Assessment of the consequences of sabotage takes into account not only direct sabotage of NM and ORM but also of SSCs that are necessary to maintain the control of FSFs and, hence, ensure nuclear safety.

32.3.4 Assumptions and Commitments

No Assumption or Commitments are raised against future Dutyholder / Licensee / Permit Holder with regard to Threat Interpretation at Version 3 of the E3S Case.

Any working assumptions made with regard to threat are recorded and collated on the RAIDO Log [10]. These assumptions will be checked and removed or managed as part of the continuing development of the Security Case. They will not necessarily become commitments on a future Dutyholder / Licensee / Permit Holder.

32.4 Secure by Design

32.4.1 Introduction

32.4.1.1 Background

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 results 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.

32.4.1.2 Relevant Tier 2 and Tier 3 Evidence

This section of Chapter 32 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 [38].
- Rolls-Royce SMR: Secure by Design Report [19].

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

32.4.2 Claims Addressed

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

[Claim 32.1] 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] A set of credible Secure by Design principles have been published and have been applied to the design of the Rolls-Royce SMR.

[32.1.2] A credible Secure by Design methodology has been applied to the design of the Rolls-Royce SMR.

[32.1.3] Security considerations are integrated into the design process.

[32.1.4] Security functions are integrated into SSCs in a way that is consistent with the operational intent of the Rolls-Royce SMR.

[32.1.5] Security risk inherent in the Rolls-Royce SMR has been minimised, prior to the application of dedicated security measures.

These sub-claims are tabulated in Section 32.13 (Appendix A), which also presents further decomposition to Level 3.

32.4.3 Features of Secure by Design

The high-level features of the SbyD approach [38] 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.

32.4.4 Secure by Design Principles

The SbyD principles (see Sub-section 32.2.3) are recorded in, and communicated to the engineering community through, the Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles [41].

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

32.4.5 Approach to Secure by Design

The Secure by Design Methodology [38] has taken account of RGP, and the experience gained to date through interaction with the maturing design.

This approach (which is outlined further in [38]) 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.

The application of SbyD is based around a Secure by Design Guidance document [42] which was produced by Rolls-Royce Civil Nuclear as part of a research contract for the (former) Department of Business, Energy and Industrial Strategy (BEIS). The research undertaken included a consultation exercise across the UK Civil Nuclear Industry to incorporate RGP. This (BEIS) guidance was an input into the development of the Rolls-Royce SMR SbyD methodology.

Although the application of SbyD is being undertaken (at Version 3 of the E3S Case) with regard to the UK regulatory regime, the intention is that the resultant (generic) security solution should be capable of deployment globally.

32.4.6 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 design features is presented in Table 32.4-1.

Table 32.4-1: Potential Security Aspects of a Compact and Modular Design

Design Feature	Potential Security Benefits	Potential Security Hazard
Berm	Hostile vehicle mitigation, Visual screening,	{REDACTED}
Hazard Shield	Nuclear material and Safety Class 1 features contained inside a substantial structure.	{REDACTED}
Shape	Greater visual coverage & more easily defensible.	{REDACTED}
Compact Site	Smaller area to defend, Fewer personnel, which makes the insider threat easier to manage.	{REDACTED}

This preliminary identification of potential benefits and vulnerabilities has (informally) informed the preliminary application of SbyD. More detailed assessment is undertaken, as appropriate within the security analyses and or in the design of the ISS.

32.4.7 Overview of the Secure by Design Methodology

The SbyD methodology is spread across three stages (see Figure 32.4-1). 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]. 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.

How SbyD integrates with the security analyses and subsequently the development of the ISS is detailed further in the SbyD Methodology [38].

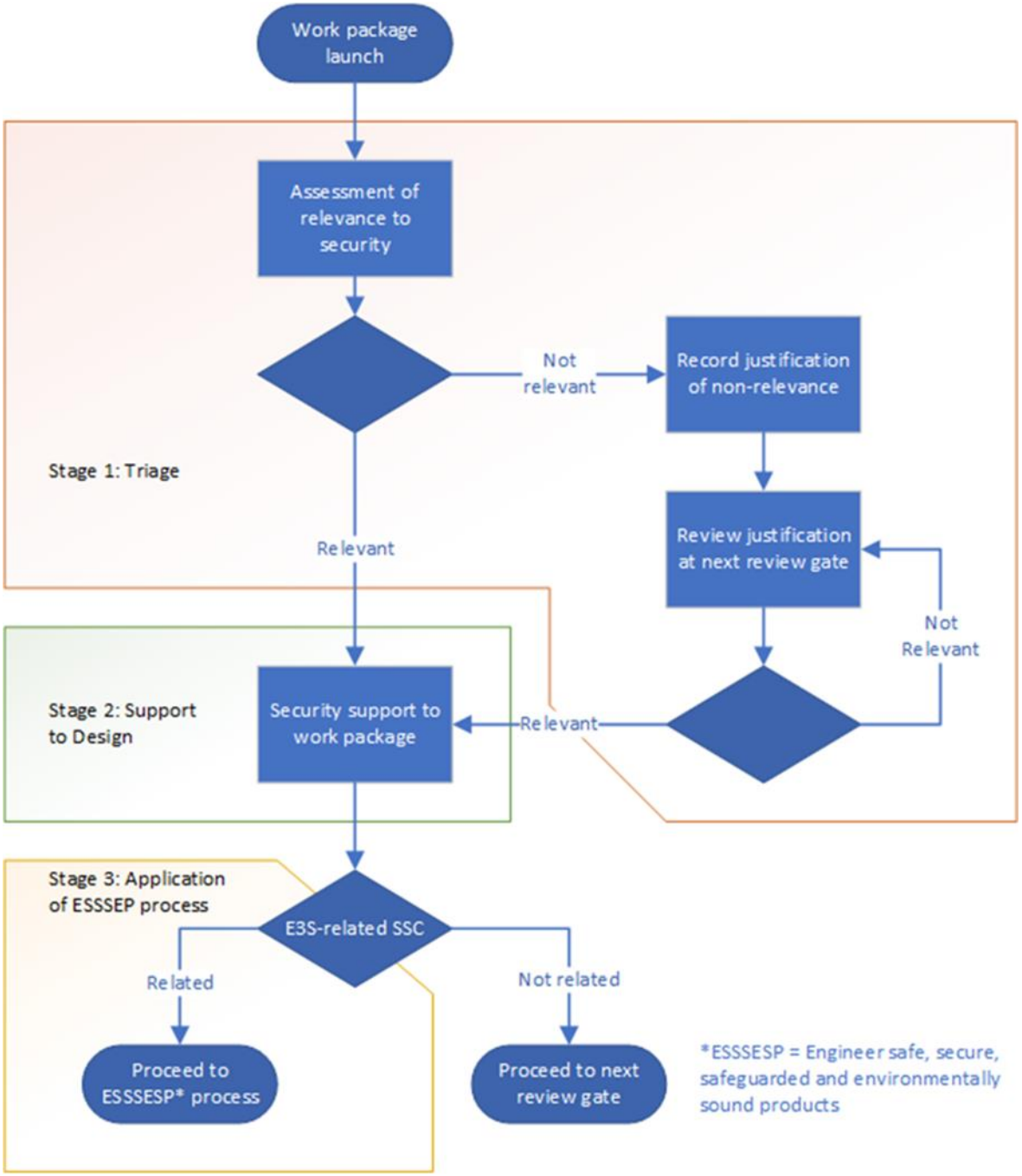


Figure 32.4-1: Secure by Design Methodology Overview

32.4.8 Security Categorisation and Classification

32.4.8.1 Introduction

The purpose of the Functional Security Categorisation and Classification Methodology [43] 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.

32.4.8.2 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 [41]. This allows for fundamental differences in how security and safety consider the frequency of potential initiating events and IEMOs. The overall approach is consistent and aligned, providing an integrated E3S approach.

Cyber security degrees (see Sub-section 32.6.4.2) 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 [44].

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.

32.4.8.3 Security Functions

32.4.8.3.1 Physical Security Functions

The physical security functions mirror those defined in the ONR SyAPs [17] and Annexes [30] and are aligned to the key functions of a physical protection system defined in international relevant good practice [24].

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

32.4.8.3.2 Cyber Security Functions

The cyber security functions are aligned with the categories of activities outlined in the ONR SyAPs [17] and the National Institute for Standards and Technology (NIST) framework for improving critical infrastructure cyber security [45].

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

32.4.8.4 Methodology to Categorise Security Functions

32.4.8.4.1 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 [30].

32.4.8.4.2 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 Annexes [30]. 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 Annexes [30]. 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.

32.4.8.5 Methodology to Classify SSCs Delivering Security Functions

32.4.8.5.1 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.

32.4.8.5.2 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: Security Class 1, which has the most stringent requirements, Security Class 2, and Security 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.

32.4.9 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 [38].

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 [46].

Further detail of this interaction is provided in the Secure by Design Report [19].

32.4.10 Security Analyses

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

- Categorisation for Theft Methodology [47].
- Cyber Security Risk Assessment Methodology [44].
- Vital Area Identification and Categorisation Methodology [48].
- Protection of Sensitive Nuclear Information [49].

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

The assessment of systems for the protection of SNI, is not covered within the current iteration of the SbyD report and will be covered in Version 5 of the E3S Case.

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).

The Manage Change IMS Process [50] requires Security SMEs to be informed of design changes, at which point an assessment made of any implications of the change on security. This might necessitate repeating the relevant security analyses.

32.4.11 Integrated Security Solution

After the issue of the ONR SyAPs [17], the regulatory regime for nuclear security in the UK has become more permissive. Dutyholders are now required to meet certain Security Outcomes and Postures [30]. These outcomes are determined from the results of security analyses undertaken to assess risk of sabotage, theft (of NM and/or 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. 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 vulnerabilities.
- Dedicated security SSCs, that is SSCs whose primary purpose is to 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 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. The development of the ISS is outlined in Section 32.8.

This ISS provides the basis for the subsequent development a Nuclear Site Security Plan (NSSP) (in UK) or similar (worldwide) (see Section 32.10). When completed, the ISS should provide a future Dutyholder / Licensee / Permit Holder 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.

32.4.12 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 [51].

At various stages of design development, reviews are conducted to ensure alignment of the design with the E3S Design Principles [37] and Requirements [52] 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 [13] that is, the overarching objective of 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 [53] 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 [52].

32.4.13 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 of the 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.

Metrics to demonstrate the interaction between SbyD and design engineering are recorded with a SbyD Database [54] (see 32.4.13.1). The initial interaction seeks to identify the SSCs with which there is a potential security risk. This potential risk is recorded in the initial SbyD assessment for the SSCs.

SbyD has sought to influence concept design and optioneering to reduce any associated security work. Details of such are recorded in the relevant engineering design documents.

As engineering design matures, security analyses assess risk and, as appropriate, made recommendations for risk requirements on design. These recommendations are recorded within the relevant security analyses documents, with a flow down of security requirements into the Rolls-Royce requirements management database.

Overall, it is not straightforward to demonstrate in detail the impact of Secure by Design; rather this will best be understood by the comparison of the ISS (for the RR SMR) against the previous security regime for nuclear power plants.

High-level examples of the impact of SbyD on engineering design (including site layout) are set out in Table 32.4-2.

Table 32.4-2: Examples of Secure by Design Input to Engineering Design and Layout

Design Feature	Secure by Design Input
Fluid system isolation valves	Advice on the location of valves in more readily secured areas.
Fluid systems pipework	Advice on locations where pipework passes through walls or other structures.
Fluid systems storage tanks	Advice on the relative location of the storage tanks.
Nuclear fuel route	Advice on security requirements for handling and movement of spent fuel and to reduce vulnerability during on-site transport.
Composite material (steel and reinforced concrete)	Layering steel and reinforced concrete in the construction of spent fuel pool provides enhanced protection against DBT sabotage capabilities
Drainage pipes and ducts	Restricting the diameter of drainage pipes and ducts under the berm prevents them being used to gain unauthorised access to the inner berm area. For drainage, multiple smaller diameter pipes are used to achieve the same flow as the large diameter pipe they replace.
Infall and outfall ponds	Location of ponds outside the berm prevents the intake and outfall tunnels being used to gain unauthorised access to the inner-berm area.
Vehicle access and internal roadways	Recommendations regarding the location and space required for vehicular access control
Access control	Recommendations on location of pedestrian access control points
Main Control Room	Advice and outline security requirements for the main control room

Evidence of the SbyD input is contained in various relevant record, including those of design reviews, HAZOPs and the security analyses workshops. How this input is actioned (or otherwise) is tracked as part of the SbyD approach.

Further details of the influence of SbyD on engineering design and layout will be provided (with references to evidence sources) in future issues of the SbyD Tier 2 report [19].

32.4.13.1 SbyD Database

A SbyD-Database [52] 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.

32.4.13.2 RAIDO Log

A Risks, Assumptions, Issues, Dependencies and Opportunities (RAIDO) Log [11] documents and tracks risks, assumptions, issues, dependencies, and opportunities during both formal security analyses, reviews, and informal engagements with engineering.

The RAIDO Log serves to evidence on-going application of the Secure by Design methodology being implemented across the project and also captures any commitments or risks that future Dutyholder / Licensee / Permit Holder be responsible for managing as they are outside the control of Rolls-Royce SMR Limited.

The RAIDO Log utilises a numbering of 32.X.YYYY, where:

- '32' represents the E3S Case Chapter.
- 'X' represents the security topic area; SbyD(1), CFT(2), CSRA(3), VAI&C (4) and ISS (5).
- 'YYYY' is consecutive numbering system for each of the individual security topic areas.

32.4.14 Conclusions and Forward Look

A framework for the application of SbyD (see Sub-section 32.4.7) has been developed which sets out a structured approach to the interaction between SbyD and engineering design and how SbyD integrates the security analyses and the development of the ISS (see Section 32.8).

This framework, which integrates the security objective (see Sub-section 32.2.2) and SbyD Principles (see Sub-section 32.2.3) into engineering design and site layout, has allowed for:

- A preliminary identification of SSCs associated with sources of the security risk, which require more detailed security analysis.
- Influence on the early concept design stage for SSCs to reduce security risk, through the application of high-level security requirements.
- Interaction with on site layout and civil engineer to build-in security and ensure that space and power is available for protective security measures.
- As the design of SSC matures (and more detailed security analysis are undertaken), more specific security vulnerabilities are idented and advice provided on advice on design modifications to such, including where appropriate specific security requirements for SSCs possible design modification and security requirements derived from security analysis work.
- The identification of residual security vulnerabilities (which cannot be addressed through design modification of engineering SSCs) that requires protective measures as part of the ISS, for example provision of access control, and intruder detection capabilities.

Application of the SbyD methodology is an on-going activity that continues in co-ordination with the maturing engineering design and layout; and will continue to be applied to a maturing and evolving design.

The evidence of the application of SbyD is shown through the application of the security analyse and the development of the ISS rather than as standalone pieces of evidence.

32.4.15 Assumptions and Commitments

No Assumption or Commitments are raised against a future Dutyholder / Licensee / Permit Holder with regard to SbyD at Version 3 of the E3S Case.

Other working assumptions made to allow the SbyD to progress are recorded in the relevant Tier 2 and Tier 3 documents and collated on the RAIDO Log [11]. These assumptions will be checked and removed or managed as part of the continuing development of the Security Case. They will not necessarily become an assumption on a Future Operator / Dutyholder / Licensee.

32.5 Categorisation for Theft

32.5.1 Introduction

The Security Case 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 [27] used to determine the levels of security that should be applied to protect the material.

This section describes 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 [47]; an overview of which is presented in this section. The categorisation addresses the following NM/ORM in its various stages through the fuel route specifically:

- Nuclear fuel –
  - unirradiated (new) fuel.
  - irradiated (used/spent) fuel.
- Intermediate Level Waste (ILW) and Low Level Waste (LLW) containing Nuclear Material.
- Discrete radioactive sources.
- Any other ORM.

In accordance with the SyAPs [17], an overall categorisation for the generic RR SMR is arrived at based on a total on-site inventory. In addition, the individual building or areas where ONM/ORM is present are also categorised. This approach allows for the design of the PPS to be specific in the location of security measures which protect against theft.

As demonstrated below the CfT with respect to the main source of NM (nuclear fuel) on the RR SMR is CATEGORY III. This categorisation is based on nuclear fuel with an enrichment of < 5 %. On this basis, this categorisation will not be subject to change as a result of aggregation.

32.5.2 Relevant Tier 2 and Tier 3 Evidence

This section of Chapter 32 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 [47].
- Rolls-Royce SMR: Theft of Material and Categorisation Report [20].

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

32.5.3 Claims Addressed

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

[Claim 32.2] Material at risk of theft is identified. Security measures are identified, and applied in a Graded Approach, to minimise the risk of theft.

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:

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

[32.23.2] The relevant security outcomes and requirement for protection for the categorised NM & ORM are established.

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

32.5.4 Overview of Categorisation for Theft Methodology

32.5.4.1 Introduction

A CfT Methodology [44] 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 in 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 [17].
- ONR Nuclear Security Technical Assessment Guide, Categorisation for Theft (CNS-TAST-GD-6.1) [31].

The starting point for this security analysis is an inventory of NM, ORM and radioactive sources that will be present (or are 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 [30].

This includes for a (whole) site categorisation and a categorisation for individual buildings holding NM, ORM or radiological sources.

32.5.4.2 Categorisation of Nuclear Materials

Categorisation of NM for theft is undertaken in line with Table 1 in SyAPs Annexes [30] 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).

The overall categorisation for the generic RR SMR is based on the total amounts held on-site

Figure 32.5-1 summarises the steps in the categorisation of NM. Further details are provided in the methodology [47].

The categorisation of the NM 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 in the ISS [23].

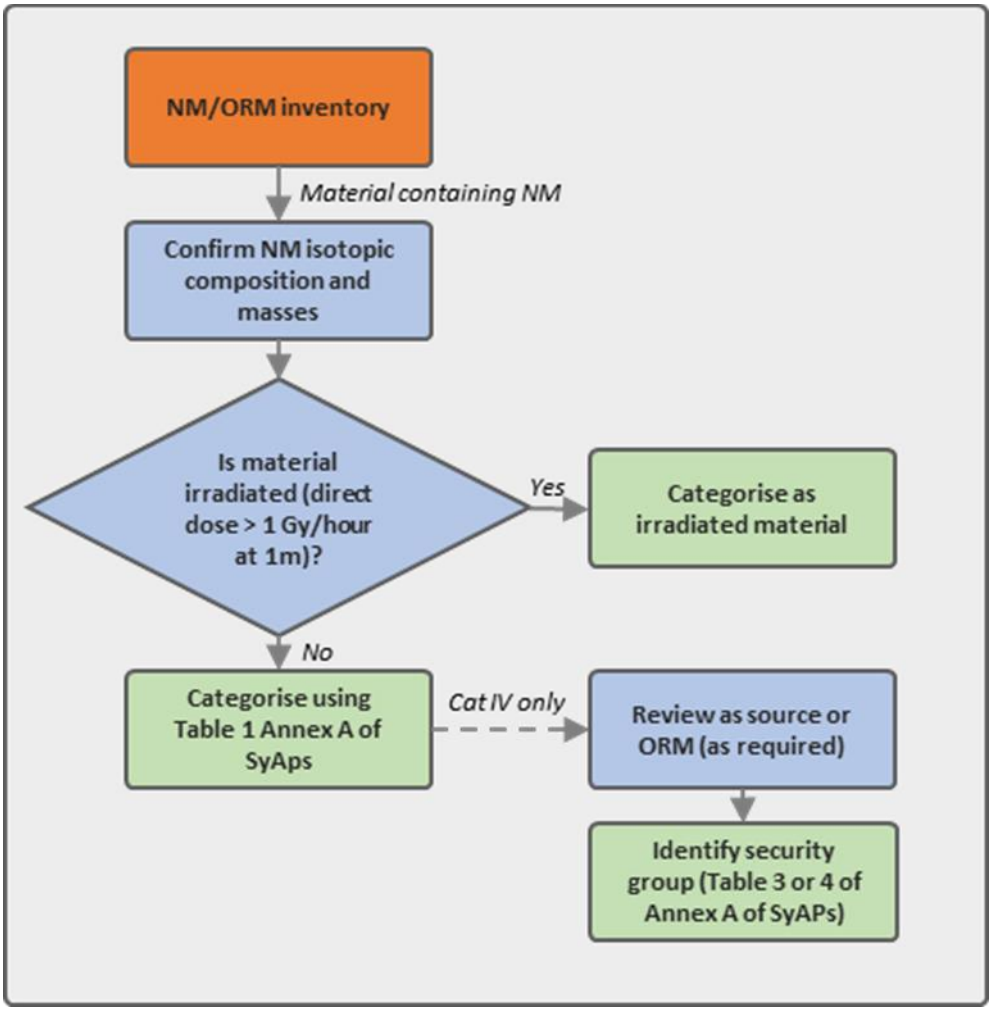


Figure 32.5-1: Categorisation of Nuclear Materials (NM)

32.5.4.3 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 secure, 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 [30] 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.

32.5.4.4 Categorisation of Radioactive Waste and Other Radioactive Materials

Radioactive waste on the RR SMR site could include ILW and LLW, for example used filters and ion exchange columns. The inventory of wastes should also consider the potential variation of this inventory during the RR SMR lifecycle which should also be considered within the categorisation process. Categorisation of ILW and LLW containing nuclear material is based on Table 2 the SyAPs Annexes [30].

A variety of ORM could be present, resulting from contamination or activation. Categorisation of ORM is based on Table 4 the SyAPs Annexes [30] and takes into account the dose rates associated with the ORM.

Figure 32.5-2 summarises the step in the categorisation of ORM. Further details are provided in the methodology [47].

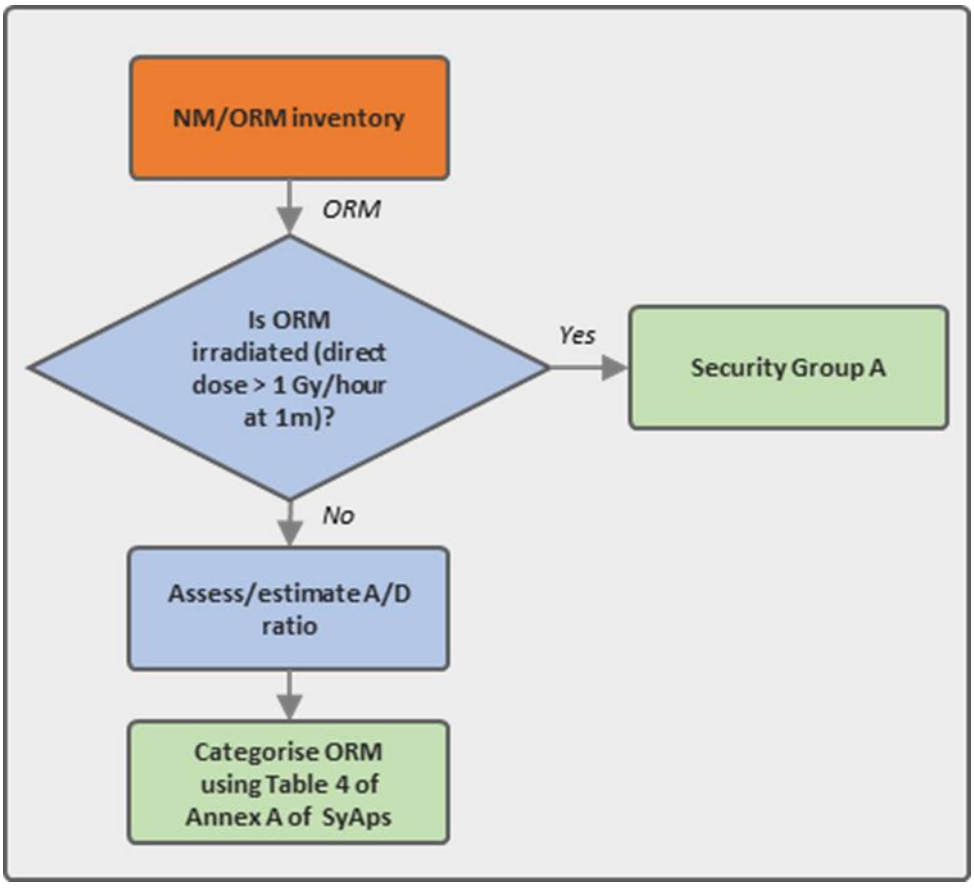


Figure 32.5-2: Categorisation of Other Radioactive Material (ORM)

The categorisation of the ILW/LLW and ORM reflects the total amount held on the site and does not reflect the ease by which the material 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.

32.5.4.5 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. This process is summarised in Figure 32.5-3.

Where an area of the plant requires protection from both theft and sabotage, the requirements are 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 is applied when considering potential vulnerabilities and potential design changes to improve robustness against theft due to design or operational changes.

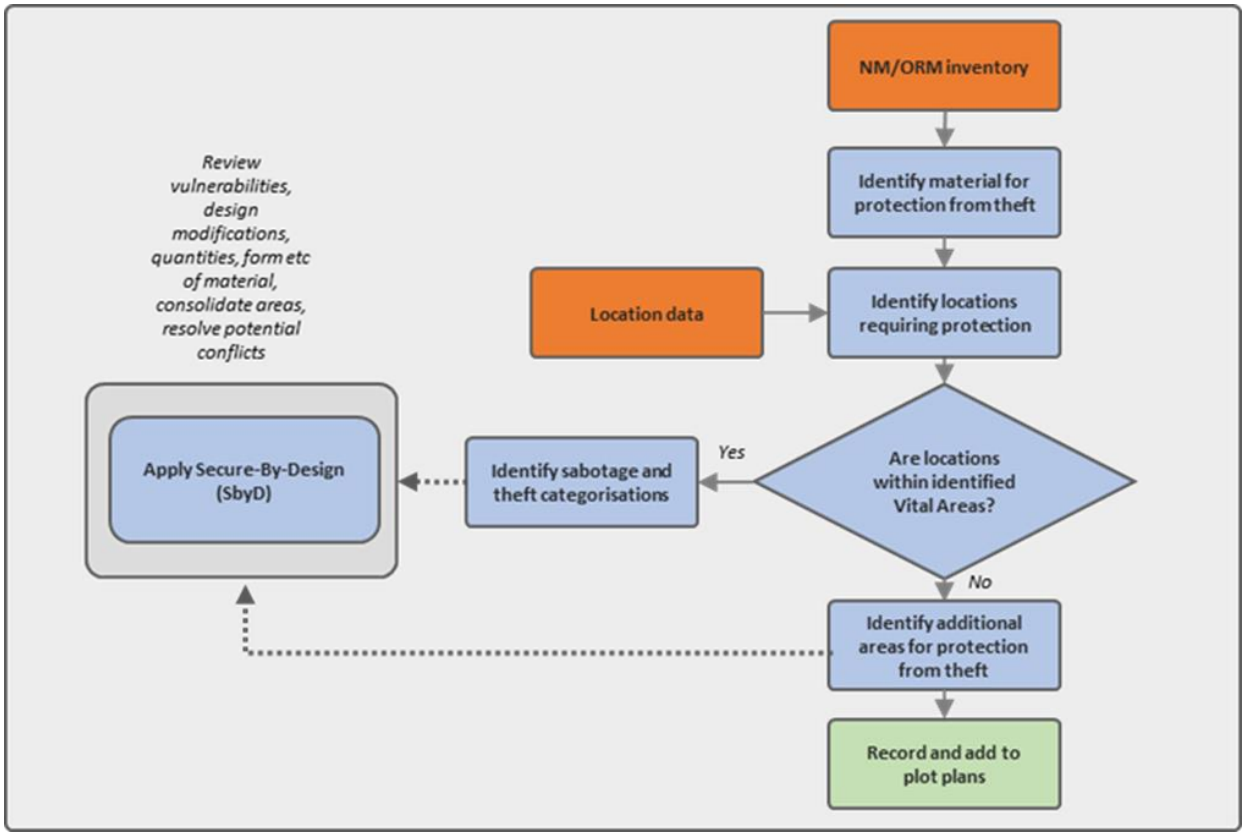


Figure 32.5-3: Identification of Theft Protection Areas

32.5.4.6 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 [38] should also be applied to ensure that robustness against theft of material is designed-in where appropriate.

Likewise, during the operation of a RR SMR, it is a responsibility of the future Dutyholder / Licensee / Permit Holder to manage any changes in the inventory of NM and ORM and review the associated CfT and associated security measures. This management of the inventory is integrated with nuclear material accountancy for the purposes of the Safeguards [14] component of the E3S Case.

32.5.5 Output from Categorisation - Nuclear Materials

32.5.5.1 Introduction

The principal source of NM associated with the RR SMR is nuclear fuel containing U-235, with an enrichment of not greater than 4.95 % contained in fuel assemblies made up from individual fuel rods and other associated components as outlined in Chapter 4: Reactor (Fuel and Core) [55].

The fuel rods within the fuel assemblies have a length of approximately 2.8 m (compared with a length for 3.6 m for that of standard fuel [55]. A standard assembly contains approximately 450 kg of uranium dioxide (UO_2).

On this basis, the approximate mass of U-235 in a RR SMR fuel assembly is as follows:

- The RR SMR fuel rod length is approximately 76 % of that of standard fuel.
- A typical a single SMR fuel assembly contains 340 kg of UO_2, which equates to 295 kg of uranium.
- For a maximum enrichment of 4.95 % for the RR SMR, each fuel assembly contains approximately 14.5 kg of U-235.

32.5.5.2 Inventory

Based on current design information regarding the fuel route [55] & [56] the inventory and locations for nuclear fuel are as presented in Table 32.5-1.

Table 32.5-1: Summary of Inventory of Nuclear Material

Nuclear Material Type	Location	Notes
Unirradiated (New) Nuclear Fuel Assemblies	Fuelling Block- Fuel Receipt and Inspection Area	Prior to each refuelling outage, up to 45 new fuel assemblies will arrive at the New Fuel Receipt and Inspection Area [56].
	Fuelling Block – Spent Fuel Pool	Prior to each refuelling outage, up to 45 new fuel assemblies will arrive at the New Fuel Receipt and

Nuclear Material Type	Location	Notes
		Inspection Area and after inspection are stored in the Spent Fuel Pool [56].
	Containment - Refuelling Pool	Prior to insertion into the core, new assemblies may be held (temporarily) in the in-containment pool
Irradiated Nuclear Fuel Assemblies	Containment - Reactor Core	For the initial fuel load the core holds 121 fuel assemblies [56].
	Containment – Refuelling Pool	Following removal from the core, spent fuel assemblies may be held (temporarily) in the in-containment pool
	Fuelling Block – Spent Fuel Pool	The irradiated assemblies are stored in the SFP for a period of 6 years prior to packing and transferring to a dry fuel storage facility. Spent Fuel Pool is designed to hold a maximum of 520 fuel assemblies (new and/or spent) [55].
	Spent Fuel Store – Dry Cask Store	Following cooling, spent fuel assemblies are placed with a storage cask which I will be transferred to a long-term store
Unirradiated (New) Nuclear Fuel Assemblies	Fuelling Block-Fuel Receipt and Inspection Area	Prior to each refuelling outage, up to 45 new fuel assemblies will arrive at the New Fuel Receipt and Inspection Area [56].

32.5.5.3 Categorisation

The categorisation of relevant NM against the appropriate criteria in Table 1 of the SyAPs Annexe [30] is shown in Table 32.5-2. This categorisation of nuclear fuel is based against the quantities of U-235 in the fuel.

Table 32.5-2: Categorisation of Nuclear Fuel

Material	Categorisation
Unirradiated U-235 at an enrichment of between 0.7 % and 10 %	For the unirradiated U-235, the quantity of U-235 in a single fuel assembly is above the threshold for Category III.
Irradiated materials	Any quantity of irradiated U-235 is categorised as Category III.

On the basis of the assumptions regarding fuel design (see Sub-section 32.5.5), a single fuel assembly (unirradiated or irradiated) is sufficient for Category III. On this basis, any location containing a fuel assembly would be Category III.

Following irradiation, the fuel will contain small amounts of plutonium (Pu). The quantity of Pu in spent fuel is not calculated, as it remains within the fuel matrix and is not separated. This approach aligns with standard industry practice; hence, no categorisation against plutonium is undertaken.

32.5.6 Output from Categorisation – Radioactive Waste

32.5.6.1 Introduction

CfT of ILW and LLW for the Rolls Royce SMR is made against the mass of plutonium or specified uranium isotopes in the waste.

The information on quantities of such in waste material is current is insufficient to accurately characterise these materials. As the design of the waste management route matures, further information will become available [56].

Ultimately, it is the responsibility of the future Dutyholder / Licensee / Permit Holder to undertake the categorisation of radioactive waste as it is generated and managed.

32.5.6.2 Inventory

ILW and LLW will be generated from a variety of sources including during normal (power generating) operation, from maintenance operations and outages or as a result of failed components [57]. The potential for contamination of these wastes with NM or ORM will depend on source.

Several of these waste streams arise from treatment of liquid wastes associated with the primary cooling circuit [57], as outlined in Table 32.5-3. These wastes have greatest potential for contamination with NM or ORM, as outlined in E3S Case Chapter 11 [57].

Table 32.5-3: Indicative Types of ILW and LLW arising from the Primary Circuit.

Waste	Physical Form	Classification
Resins (Chemistry Volume and Control System)	Wet	ILW
Suspended filter solids	Wet	ILW
Evaporator concentrates	Wet	Boundary ILW/LLW
Resins	Wet	Boundary ILW/LLW

The contamination of waste streams with U-235 should only occur as a result of cladding failure. As the enrichment in the fuel will be < 4.95 %, then enrichment in waste will not exceed 5 %. Therefore, the likely material categorisation for contamination by U-235 will be via Table 1 rather than Table 2 of the SyAPs Annex [30]. This would result in a categorisation as either Category III or Category IV, depending on the quantity present.

Likewise, contamination of waste by plutonium will only occur as a result of compromise of fuel cladding and release into the primary circuit, from where it could transfer into relevant waste streams.

ILW and LLW will be collect and treated within the Waste Block, prior to packaging for longer-term storage.

Once processed and packaged, ILW will be contained in a shielded storage facility in the waste block designed to maintain the condition of packaged ILW in a manner that protects workers, the public and the environment from hazards associated with interim storage until the waste can be transported to a future Geological Disposal Facility (GDF) [58].

32.5.6.3 Categorisation

Categorisation of contaminated ILW and LLW is best undertaken as the wastes are generated and treated in association with accurate characterisation of waste stream in conjunction with their management and disposal.

For current purposes, an assumption is made that (under normal operational circumstances) the categorisation of waste material will not lead to an overall CfT of greater than Category III; nuclear fuel will be the primary driver for CfT. This will be confirmed or otherwise as further relevant information becomes available.

32.5.7 Output from Categorisation – Discrete Radioactive Sources

At Version 3 of the E3S Case, there is insufficient information to determine the type and location of Discrete Radioactive Sources, and no final decisions have been made regarding these aspects. This will be addressed at a later stage when more information becomes available and will include considerations for start-up neutron sources and Self-Powered Neutron Detectors (SPND).

Categorisation for Theft for discreet radioactive sources is undertaken against the criteria in Table 3 of SyAPs Annexes [30] and IAEA General Safety Guide No. RS-G-1.9 [59].

32.5.8 Output from Categorisation – Other Radioactive Materials

Categorisation is based on dose rate emitted from the ORM. This could result from contamination by radioactive material or activation as a result of exposure to radiation (primarily neutron flux). ORM could include ILW/LLW which is contaminated but not by nuclear materials in (amounts sufficient to trigger Categorisation for Theft.)

Potential dose rates are difficult to predict. Hence, as for ILW/LLW containing NM, the Categorisation of ORM is best undertaken in 'real time' in association with accurate characterisation of in conjunction with their management and disposal. For activated materials, this is most likely to be of relevance as a result of maintenance activities or during decommissioning.

Various pathways may generate ORM. Current information is insufficient to support the development of an inventory or its characterisation. Further consideration of the presence and location of ORM will be made in in conjunction with the development of arrangements for waste management and decommissioning.

32.5.9 Integrated Security Solution

32.5.9.1 Introduction

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. and includes:

- The categorisation for theft.
- The location where the NM and ORM is located (including whether co-located with a vital area).

32.5.9.2 Secure by Design

In alignment with the SbyD approach, 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 or reduce the categorisation of the material within a particular area.

The amount of nuclear fuel (new and spent) present is optimised for power generation efficiency. As such there is limited potential to reduce the amounts of fuel present. Furthermore, as categorisation is against a single fuel assembly, reduction in amount would not impact on the Categorisation for Theft.

The security requirements to protect against theft of ILW, LLW and ORM will take into account the volumes involved.

E3S Case Version 3, Tier 1, Chapter 11: Management of Radioactive Wastes [57] set out how the application of BAT is used to minimise the volume of radioactive waste generated and ensure that such can be safely handled and stored. The application of BAT aligns with the SbyD approach through partial elimination and substitution (see Figure 32.2-1).

32.5.9.3 Physical Protection System

The protection afforded to the identified NM/ORM (and the areas where they are located) is graded depending on the sabotage-related consequential dose or the NM, ORM or sources located within them, as follows (based on Annex C of the SyAPs Annexes [27]).

- 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 outcome associated with the theft categorisation applies.

32.5.10 Conclusions and Forward Look

The CfT analyses identify the NM (nuclear fuel) which requires protection against theft. The Categorisation of this fuel is Category III for both irradiated and non-irradiated fuel. The is based on the reactor core design which utilises nuclear fuel with an enrichment <5 %.

Categorisation of waste material is not expected to challenge this categorisation for the site-wide inventory as a whole. Likewise, the quantities of fuel (and waste) are not expected to result in an increased categorisation as a result of aggregation.

The potential for other material to require protection is identified at a high-level; and requires confirmation or otherwise on further data is available regarding confirmation of material characteristics.

The CfT (outlined in this Section) is taken forward into the ISS through the identification of the appropriate Security Outcomes and Postures from the ONR SyAPs Annexes [30].

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 categorisation does not take into account the characteristic of the material (for example physical and chemical form), the protection provided by engineering design, nor the capability required by the threat. This is addressed as part of the design of the ISS, which will co-ordinate requirements for protection from both theft and sabotage as part of the integrated whole.

The application of the CfT methodology is not intended to be a one-off but rather an iterative process. The CfT outlined above will be kept under review as the engineering design and layout matures and the categorisation revised as necessary.

32.5.11 Assumptions and Commitments

The following Assumption or Commitments are raised against a future Dutyholder / Licensee / Permit Holder with regard to CfT:

- [Commitment-32.2.0003] A future Dutyholder / Licensee / Permit Holder should identify and characterise all ILW/LLW as it is generated to facilitate accurate categorisation for theft.
- [Commitment-32.2.0004] A future Dutyholder / Licensee / Permit Holder should identify and characterise all ORM that is generated to enable appropriate categorisation for theft.

Other working assumption made to allow the CfT to progress are recorded in the relevant Tier 2 and Tier 3 documents and collated on the RAIDO Log [11]. These assumptions will be checked and removed or managed as part of the continuing development of the Security Case. They will not necessarily become an assumption on future Dutyholder / Licensee / Permit Holder.

32.6 Cyber Security

32.6.1 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:

- Computer-based Systems that are associated with structures, systems and components (SSCs) the sabotage of which that could result in an Unacceptable Radiological Consequence (URC). In the UK, these systems are commonly referred to as Computer Based Systems Important to Safety (CBSIS).
- Computer-based Systems that protect against the theft of nuclear material or sabotage against nuclear material or nuclear systems that could credibly result in an URC. In the UK, these systems are commonly referred to as Computer-Based Security Systems (CBSy).
- Computer-based Systems that are essential to generation of electricity and transfer to external grid systems.
- Understanding and assessing cyber risks is essential to the selection of appropriate inherent and mitigating security controls, protecting safe and secure operations from potential cyber risk.

This Security Case does not specifically differentiate between these types of systems; hence, reference to Computer-based systems in this section (and in discission of a CPS) includes for all the sub-sections listed above.

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 [44], an overview of which is presented in this section.

The CSRA interacts with the design of the C&I systems at multiple stages. This ensures that security is considered throughout the design process, generating opportunities to apply the SbyD and, hence, reduce consequences. Systems receive cyber security requirements in three different ways:

- Security Degree Requirements: Each system is assigned a security degree during the High-Level Risk Assessment. The generic security controls associated with security degrees are described in the Cyber Security Design Requirements Specification [60].

- Functional Requirements: The design of the Cyber Protection System will identify where architectural security controls are needed to meet the CPS Outcomes. These are security functions and will be assigned to specific systems. Any system that has been assigned at least 1 security function will be assigned a security class.
- System Specific Requirements: During the Zones and Conduits Assessment or the Detailed Risk Assessment, it may be identified that the security degree requirements are not sufficient to reduce the risk to an acceptable level. In this case, system specific requirements will be proposed by the security team in alignment with the design team.

32.6.2 Relevant Tier 2 and Tier 3 Evidence

This section of Chapter 32 summarises the CAE relevant to the topic area 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 [44].
- Rolls-Royce SMR: Cyber Security Report [21].

These Tier 2 documents reference Tier 3 sources of evidence, including that relating to the application of the methodology. This includes (to date) reports presenting the CSRA for the following systems:

- Reactor Protection System (RPS) [JRA][2].
- Diverse Protection System (DPS) [JQA].
- Reactor Plant Control System (RPCS) [JSA].
- Data Processing and Control System (DPCS) [CB].

32.6.3 Claims Addressed

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

[Claim 32.3] Effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology (including Information Technology (IT) and Operational Technology (OT)) have been implemented and maintained.

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] – A cyber protection system, including policies and procedures, is in place to manage cyber risk in accordance with recognised international standards and RGP.

[32.3.2] – Computer-Based Systems are risk assessed using a consequence-based risk assessment process and assigned a security degree.

[32.3.3] – Mitigations to cyber security risks are proportionally applied using a graded approach

[32.3.4] - The effectiveness of the cyber protection system is verified and validated

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

[2] Reference designation for SSCs within the RR SMR power station scope is implemented in accordance with the Standard Reference Designation System for Power Plants (RDS-PP®). Within the E3S Case, SSCs are referred to by their RDS-PP® code using one or more capital letters enclosed within a square bracket '[XX]'.

[32.3.6} – The Cyber Protection System, as part of the ISS, includes measures to ensure that systems are designed to be secure and resilient against the cyber threat, as defined by the DBT, throughout their lifecycle stages.

{32.3.7] The CPS provides the software, tools and architecture to enable detection, response and recovery from cyber incidents

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

32.6.4 Overview of Cyber Security Risk Assessment Methodology

32.6.4.1 Introduction

A Cyber Security Risk Assessment Methodology (CSRAM) [44] 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. Requirements for further improvement and clarification of the methodology are recognised as the methodology is applied; and the methodology will be reviewed and updated as required.

The objectives of the CSRAM are:

- Risk Identification: This identifies cyber risk through a consistent - process. This is based on the industrial cyber security risk assessment standard, IEC62443-3-2 [61] 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 by the Design Basis Threat (DBT), interpretation of the threat and consequence analysis.
- Risk Treatment: The risk scores are subject to a consistent risk treatment process to achieve the desired outcomes from ONR Security Assessment Principles (SyAPs) [30].
- Risk Management: Manages and documents the ownership of cyber risk through the life cycle of the plant as ownership transfers from designers through to future operators.

The cyber security risk assessment methodology will interface with the design at multiple stages to identify and reduce risk, as per the SbyD Methodology [38]. Each system is assigned a security degree and a graded set of baseline security controls. Where the CSRAM identifies that the baseline requirements have not sufficiently reduced the risk or the system cannot comply, the CSRAM will suggest design changes that will mitigate cyber security risk further.

Cyber security controls are subject to review to identify any safety / security conflicts and ensure compatibility with the C&I design.

Residual risk levels (with the implementation of the control sets in place and any agreed design changes) are defined and deterministic justification provided to confirm that the risk appetite / Cyber Protection System (CPS) Outcomes have been achieved in the context of each system. Where claims are made across multiple systems, then a deterministic justification is provided based on the risk levels of individual systems and any potential inter-dependencies between the systems under consideration. Residual risk levels are recorded within the safety case to ensure that the security residual risks do not prejudice the safety case claims.

The CSRAM is a modular assessment which is repeatable over the life cycle of the RR SMR. The CSRAM comprises:

- Systems Level Risk Assessment Methodology.

- Multi-Systems Threat Modelling.

Summary details are provided below, with greater detail provided in the Tier 2 methodology document [44].

32.6.4.2 Assignment of Security Degrees

BS EN IEC 62645 [62] establishes a requirement to classify C&I systems according to the maximum consequences of a successful cyber-attack on this system in terms of plant safety and performance. Rolls-Royce SMR Ltd has adopted this methodology and developed it (as shown on Table 32.6-1) with regard to assignment of Security Degrees. This table considers other potential sources of high consequence events, such as security, environmental safety, conventional safety and loss of generation. The security degree is assigned at the end of the High-Level Risk Assessment (Phase 1c).

The Security Degree is used to determine the applicable security controls. S1 implements the most stringent controls. There is also a set of Baseline Requirements which apply to all systems. Where a system has multiple classifications that would map it to different degrees, the worst case degree (lowest applicable Security Degree number) is assigned.

The security degree approach assigns a minimum security degree for the system, the security degree may be increased if it is judged during the high-level risk assessment or the Zones and Conduits Phase that the security arrangements should be enhanced.

Table 32.6-1: Security Degree Assignment Approach

Security Degree	Approach
SD1	Safety Class 1 Computer-Based systems - any [Computer-Based system] that forms a principal means of fulfilling a Safety Category A function. or - Security Class 1 Computer-Based systems - any [Computer-Based system] that forms a principal means of fulfilling a Security Category A function.
SD2	Safety Class 2 Computer-Based systems - any [Computer-Based system] that makes a significant contribution to fulfilling a Safety Category A function or forms a principal means of ensuring a Safety Category B function. or - Security Class 2 Computer-Based systems - any [Computer-Based system] that makes a significant contribution to fulfilling a Security Category A function or forms a principal means of ensuring a Security Category B function. or - Computer-Based Systems that play an essential role in the generation of power Computer-Based Systems that are essential to generation of electricity and transfer to external grid systems. or - Computer-Based systems with a high environmental protection function. Failure to implement or implement correctly could lead to a detrimental environmental consequence or breach of future permit conditions

Security Degree	Approach
	or - Computer-Based systems with direct and immediate impact on conventional health and safety.
SD3	Safety Class 3 Computer-Based Systems - any other SSC contributing to a safety categorised function. or - Security Class 3 Computer-Based Systems - any other SSC contributing to a security categorised function. or - Essential OT systems that are necessary for the generation of revenue (Metering/Billing etc). or - Computer-Based systems with a medium environmental protection function. System doesn't directly provide an environmental protection function, but could generate operational wastes and discharges which need to be controlled and therefore could impact ability to demonstrate BAT. or - Computer-Based systems that indirectly support conventional health and safety
No Degree (Baseline Requirements Apply)	Any other Computer-Based system.

32.6.5 System Level Risk Assessment Methodology

32.6.5.1 Introduction

The system level methodology has been developed to align with the requirements from IEC62443-3-2 [61] and has been tailored to meet the needs of Rolls Royce SMR. The overall system-level cyber security risk assessment methodology for systems is presented within Figure 32.6-1.

Each system level risk assessment demonstrates the evidence to justify that individual systems are secure by design and meet regulatory requirements. Importantly, it contributes to the overall justification of product safety, as if the systems within the product design are not secure, we cannot be certain that they are safe. The single systems methodology also collates information for any subsequent application of the multi-systems methodology.

Systems that are to be assessed with the CSRAM are identified by the Secure by Design methodology Initial Security Assessment, this identifies systems that need further review by the Security team. The CSRAM covers Steps 1 and 2a and 2b of the Secure by Design methodology for systems that require cyber security risk assessment.

The CSRAM Report Document is a living document that collates information from each phase of the assessment. This will mean that there is only one document per system, but that it is updated with new information as the assessment progresses through the phases.

32.6.5.2 Early Engagement – Identify System under Consideration

This phase conducts a High Consequence Event (HCE) review of the SuC, this considers potential incidents that would result in an impact that would be unacceptable to Rolls-Royce SMR Limited or the SMR Asset Owner/Operator.

Identifying the System under Consideration (SuC) focusses the cyber security risk assessment effort onto the SuC to develop a fuller understanding of the system, its dependencies, and interconnections in preparation for the High-Level Risk Assessment.

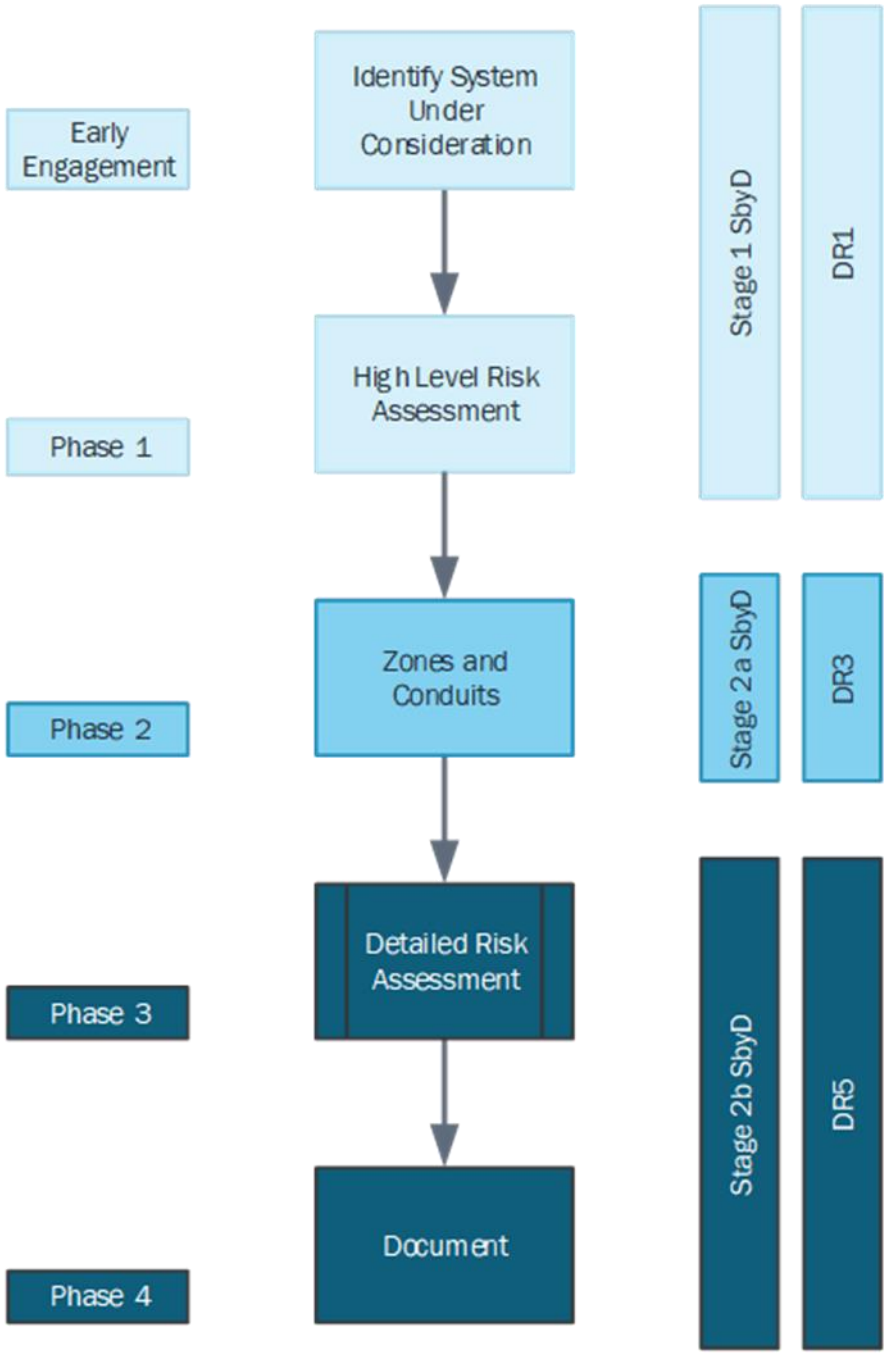


Figure 32.6-1: System Level Risk Assessment Methodology

32.6.5.3 Phase 1 High-Level Cyber Security Risk Assessment

The HCE are identified in a workshop(s) attended by personnel that meet the descriptions in the phase inputs above. A HAZOP or similar assessment must already have been completed prior to the HCE workshop, the record of the HAZOP should be used to capture safety related HCE in advance of the workshop and fed into the 'Define initial HCEs' phase.

The review is based on a defined set of boundaries, typically this is the same as the SuC. The following should be considered and recorded when defining the review boundaries.

32.6.5.4 Phase 2 – Zones and Conduits

To facilitate the detailed risk assessment, the SuC is divided into zones that contain assets with similar consequences and security requirements. This allows risks to be considered for the zone as a whole, rather than every asset within the zone, greatly simplifying the analysis. Interfaces between zones are further identified as "conduits" for transferring data between zones.

32.6.5.5 Phase 3 – Detailed Risk Assessment – Identify Attack Paths

This phase performs the detailed risk assessment on those systems that after the zones and conduits assessment, have been shown to have one or more cyber risks with a risk ranking above tolerance.

It systematically assesses each zone, conduit, and physical location to identify valid complete attack paths. Then, for each attack path, it will evaluate if current design mitigations are sufficient, and if not, propose additional compensating countermeasures.

32.6.5.6 Phase 4 – Documentation

This phase seeks to present the results of the risk assessment process at all phases.

- Residual risk levels for the SuC.
- Justification of the acceptability of residual risk from a security perspective.
- Justification that CPS outcomes have been achieved for the system under consideration.
- Identification of risk shortfalls and associated potential design changes (to be entered into the SbyD Process.
- Identification of claimed security control sets associated with the system under consideration (to be entered into the SbyD process for consideration of conflicts with the safety case, and compatibility with the C&I Design / Support System Design).

32.6.6 Multiple Systems

The defence in depth concept typically ensures that multiple systems must fail in order to generate a significant radiological release. As such, the cyber security assessment considers the cases where multiple computer-based systems must be compromised in order to generate a URC or theft event.

Typically, multi-system threat modelling approach is undertaken against a complete design. However, this does not support the secure by design approach. Therefore, Rolls-Royce SMR Limited chooses to conduct multi-system threat modelling as early as possible in the design process. This requires combining results from system-level assessments to analyse potential multi-system attack paths. This approach is shown diagrammatically in Figure 32.6-2.

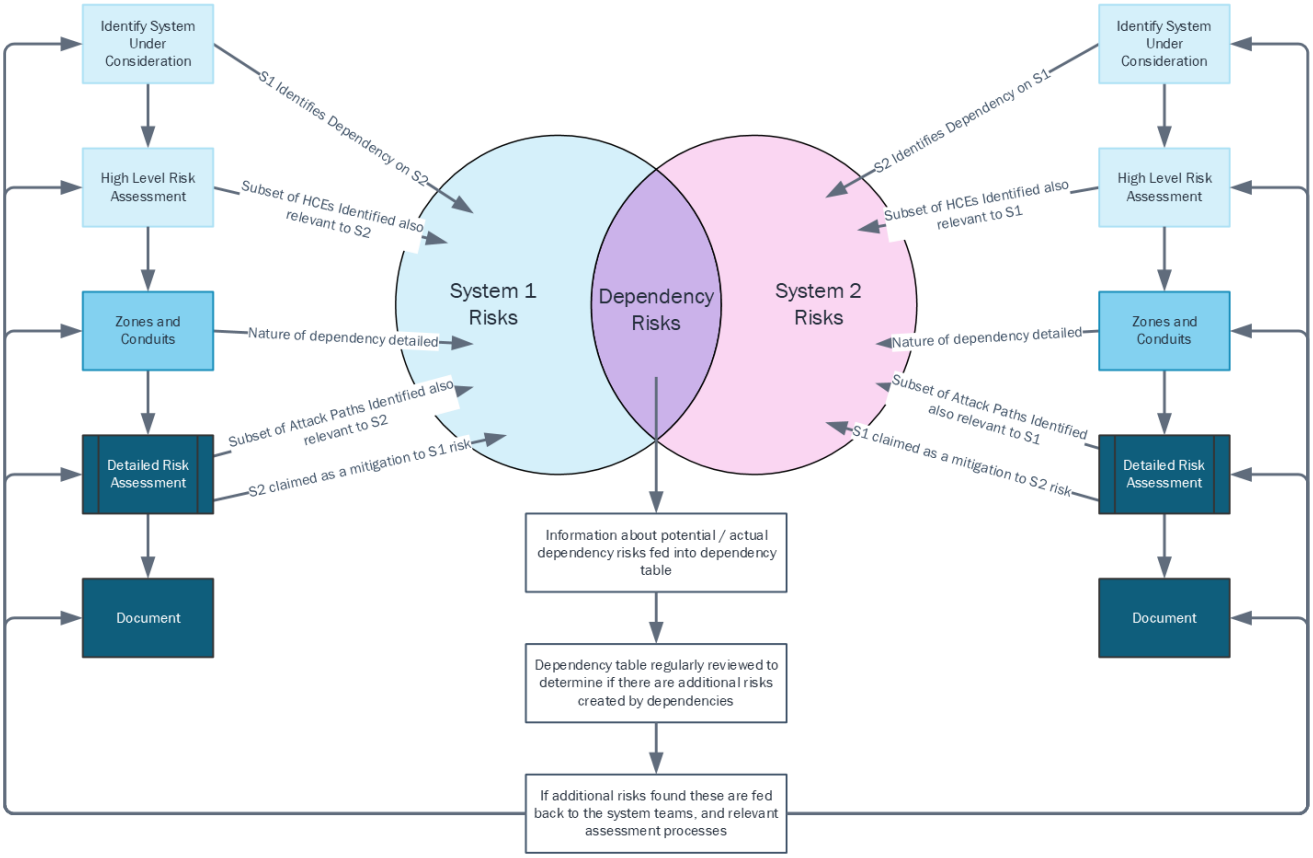

Identify System Under Consideration
High Level Risk Assessment
Zones and Conduits
Detailed Risk Assessment
Document
S1 Identifies Dependency on S2
Subset of HCEs Identified also relevant to S2
Nature of dependency detailed
Subset of Attack Paths Identified also relevant to S2
S2 claimed as a mitigation to S1 risk
System 1 Risks
Dependency Risks
System 2 Risks
S2 Identifies Dependency on S1
Subset of HCEs Identified also relevant to S1
Nature of dependency detailed
Subset of Attack Paths Identified also relevant to S1
S1 claimed as a mitigation to S2 risk
Identify System Under Consideration
High Level Risk Assessment
Zones and Conduits
Detailed Risk Assessment
Document
Information about potential / actual dependency risks fed into dependency table
Dependency table regularly reviewed to determine if there are additional risks created by dependencies
If additional risks found these are fed back to the system teams, and relevant assessment processes

Figure 32.6-2

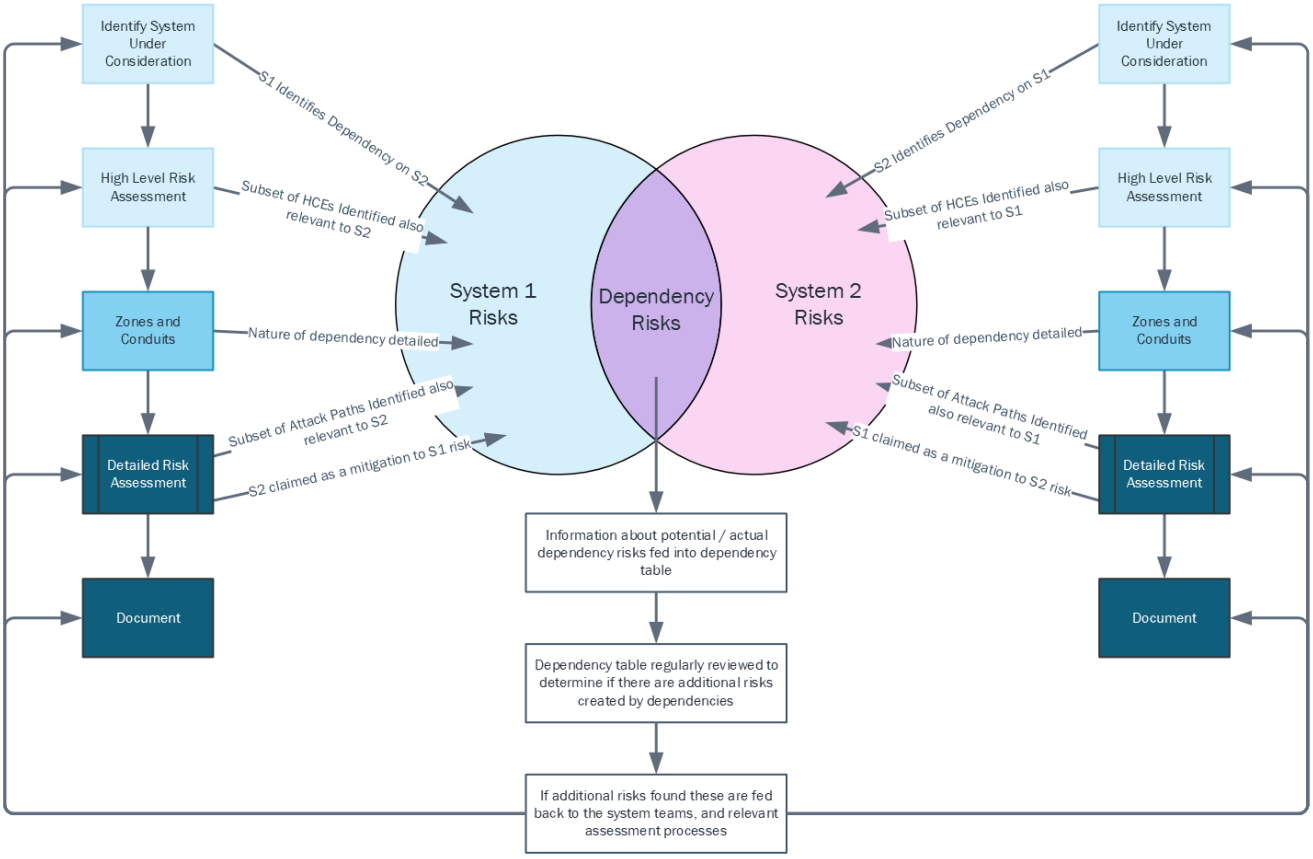

Identify System Under Consideration
High Level Risk Assessment
Zones and Conduits
Detailed Risk Assessment
Document
S1 Identifies Dependency on S2
Subset of HCEs Identified also relevant to S2
Nature of dependency detailed
Subset of Attack Paths Identified also relevant to S2
S2 claimed as a mitigation to S1 risk
System 1 Risks
Dependency Risks
System 2 Risks
S2 Identifies Dependency on S1
Subset of HCEs Identified also relevant to S1
Nature of dependency detailed
Subset of Attack Paths Identified also relevant to S1
S1 claimed as a mitigation to S2 risk
Identify System Under Consideration
High Level Risk Assessment
Zones and Conduits
Detailed Risk Assessment
Document
Information about potential / actual dependency risks fed into dependency table
Dependency table regularly reviewed to determine if there are additional risks created by dependencies
If additional risks found these are fed back to the system teams, and relevant assessment processes

Figure 32.6-2: Multi System Threat Modelling

Throughout the individual system risk assessments, information is being added to a Dependency Table. In early assessment phases, this will just be an acknowledgement that a system has a dependency, whether physical, networked, logical or otherwise, on another system but as the assessment progresses more detail is added that describes the dependency, and any identified risks relating to it.

The dependency tables developed in each individual assessment will also be recorded in a Central Dependency Table (CDT) maintained by the Security Case team. This CDT is a repository of information about all dependencies from all cyber security assessments.

Risks that are identified through the CDT and passed to individual system assessment, are analysed for controls within the individual assessments. This means that all risk related cyber security requirements will follow a common flow of Risk Assessment CPS Requirements System Requirements.

32.6.7 Integration with Secure by Design Approach

Application of the SbyD methodology [38] 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 are triggered after an initial assessment of an engineering work package is undertaken within Stage 1 Step 1 of the SbyD Methodology [15]. 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 [38]). 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 [44].

Stages 2 and 3 of the SbyD Methodology are implemented during the detailed assessment phase of the CSRAM methodology.

32.6.8 Outputs from Cyber Security Risk Assessment

32.6.8.1 Introduction

The Rolls-Royce SMR Cyber Security Report [21] summarises the progress made so far in the development of the CPS and the application of the CSRAM. It also summarises the work that will be presented by the end of GDA, and future plans to complete the generic design.

To date, the SbyD approach, at Version 3 of the E3S Case, has identified seven systems that may require CSRAM assessment. These are as follows:

- Reactor Plant Control and Protection System (RPCPS) - This is not a control system, but rather an architectural overview of Reactor Island systems. The approach to be taken for the RPCPS is to assess the individual systems.
- Fuel Route Systems and Radioactive Waste Management Systems – the maturity of these systems is not yet sufficient for a meaningful assessment. As for the RPCPS, these systems are architectural and maybe benefit from assessment via the individual systems.
- The RPS [JRA], DPS [JQA], RPCS [JSA] and DPCS [CB] have been subject to CSRA Details of these assessments are summarised in the Tier 2 Cyber Security Report [21].

Further detail of the assessment for RPS, DPS, RPCS and DPCS is provided in the individual assessment reports for the systems. The individual Tier 3 reports are:

- Rolls-Royce SMR: Reactor Protection System Cyber Security Risk Assessment Report [63].
- Rolls-Royce SMR: Diverse Protection System Cyber Security Risk Assessment Report [64].
- Rolls-Royce SMR: Reactor Plant Control System Cyber Security Risk Assessment Report [65].
- Rolls-Royce SMR: Data Processing & Control System Cyber Security Risk Assessment Report [66].

The High-Level Risk Assessment (CSRA Phase 1) and Zones and Conduits Assessment (CSRA Phase 2) have been run for these four systems. Safety Function and Fault Study information was not sufficiently mature to allow for the initial identification of attack pathways (i.e. the connections between systems and how users interact with systems).

The Detailed Risk Assessment and the Dependencies Analysis (CSRA Phase 3) have not yet been undertaken; the designs are not sufficiently mature for a meaningful output for these CSRA phases. These assessment reports will be updated as the remaining phases are completed.

Based on the assigned security degrees, a baseline set of security controls is assigned to the C&I engineers and incorporated in the detailed design of C&I Systems. This detailed design is the subject of CSRAM Phases 3 & 4, which will identify if there is a need for additional system specific security controls. Details of these controls are presented in the relevant Tier 3 analysis reports.

The CSRA was conducted against the relevant engineering design declared for DRP3, before engineering change ECR-000049. Further details of design maturity are provided in the individual Tier 3 reports.

The accepted architectural change to RPS and DPS at DRP4 requires a revision to the assessments for both. For DPS, it is unlikely to result in any significant changes, as DPS had already been allocated security degree 1. For RPS, it will likely require the zone boundaries to be changed, such that RPS 1 and RPS 2 are in different zones, and can be allocated different security degrees. Therefore, RPS 1 will have an enhanced profile of security requirements. The following sections summarise the outputs of those reports from before the architectural change.

32.6.8.2 Reactor Protection System [JRA]

The RPS is a (safety) Class 2 computerised system. The primary function of the RPS is to provide implementation of Category A & B safety functions safety functions. The RPS is a sub-system of the RCPCS.

The RPS provides:

- A diverse implementation (together with the DPS) of all Category A safety functions (RPS subsystem 1).
- The sole implementation of Category B safety functions (RPS subsystem 2).

Three zones have been defined; all three of which are assigned a SD2 security degree [63]. This security degree is assigned on the basis of the RPS as a Class 2 system that makes a significant contribution to a Category A safety function.

Numerous security dependencies have been identified. These include with DPS, RPS power supplies, RPS field instrumentation and software development environments.

32.6.8.3 Diverse Protection System [JQA]

The DPS is a safety Class 1 protection system. The primary function of the DPS is to provide Category A safety functions, by diverse means, to the Class 2 Reactor Protection System. The DPS is a sub-system of the RCPCS.

The DPS is mainly a hardwired system. The CSRA has been applied to the computer based elements of the DPS. Additionally, some of the security controls will be applicable to the hardwired DPS.

Four zones have been identified, which are assigned security degrees as follows [64]:

- Two zones are assigned a SD1 security degree, on the basis that these zones contain a Class 1 control system which makes a significant contribution to a Category A safety function.
- Two zones are assigned a SD2 security degree, on the basis that the associated subsystems of the DPS are Class 2 safety systems and the connection between the SD1 & SD2 zones is a hardware enforced unidirectional link.

Numerous security dependencies have been identified. These include with DPS power supplies, DPS field instrumentation and software development environments.

32.6.8.4 Reactor Plant Control System [JSA]

This is a safety Class 3 system. The RPCS is a subsystem of the Reactor Plant Control and Monitoring System (RPCMS). During abnormal operating conditions, the RPCS delivers preventative functions designed to restore the primary reactor systems and associated heat exchangers to their normal operating conditions without actuating the reactor protection functions or other engineered safety features.

A single zone has been assigned an SD2 security degree [65]. Although the RCPS is a Class 3 system, the HCE assessment identifies the importance and consequences of loss of the system, particularly to power generation.

Numerous security dependencies have been identified. These include with RCPS power supplies, heating, ventilation & air-conditioning (HVAC) and software development environments.

32.6.8.5 Data Processing & Control System [CB]

The DPCS is a safety Class 3 system. The DPCS is the duty control system for the RR SMR. It includes the Supervisory Control and Data Acquisition (SCADA) System [CB], the Automation and Sequence Control System [CC], the Diagnostics System [CD], the Engineering System [CE], OT networks system [CF] as well as the majority of the Class 3, Non-Classified, and duty plant control systems in the RR SMR.

Six zones are assigned a SD2 security degree [66]. Although the DPCS is a Class 3 system, the HCE assessment identifies the importance and consequences of a loss of DPCS, particularly to energy generation,

Numerous security dependencies have been identified. These include with DPCS power supplies, HVAC and software development environments.

32.6.9 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 [30] which in turn identifies the requirements for the CPS.

The ONR SyAPs (Reference [3]) define CPS outcome levels based on the threat actor skill level and the consequences of compromise of the system. The CPS outcomes define the expected response and robustness of that response against the threat actors described in the DBT.

The CSRA allocates control sets to systems and provides evidence to allow a deterministic justification that the CPS outcomes have been achieved.

While the CPS outcomes must be achieved, Rolls Royce SMR Limited, or the customer we are supplying to, may have a different attitude to risk that needs to be considered i.e. they may choose to be more conservative than the regulation requires. Risk appetite refers to the level of risk that an organization or individual is willing to accept while pursuing its objectives.

32.6.10 Conclusions and Forward Look

The CSRA identifies the cyber risk to the operation of the RR SMR. The CSRA is undertaken against a threat profile based on the UK DBT; and includes for both an insider threat and a blended attack.

The CSRA identifies requirements on digital system design and hardware (to reduce risk) and/or requirements for dedicated security measures to address the residual risk. These requirements are for security measures which deliver cyber security functions; and, for physical security measure to protection access to digital systems. Security requirements are captured within the Rolls-Royce SMR Limited requirements management database [10].

There is no strict prioritisation system for the CSRA. Systems are being assessed when their designs are sufficiently mature, which has been a steady flow so far. A prioritisation system can be introduced if this changes. The CSRAM has been designed to lag the safety risk assessments, however, only the reactor island systems have been assessed by safety so far.

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 or changes to DBT or other threat intelligence.

CSRA is undertaken in close association with the design of C&I systems [4]; and the integration of CPS requirements within the C&I design. This approach provides assurance that the C&I design is secure. This is achieved through the specification of an initial set of baselines controls to be included in the C&I designs with a requirement for addition specific controls identified as the maturing designs are considered by the later phases of the CSRAM.

The output of CSRA (outlined in this Section) is taken forward into the ISS [23] which demonstrates that the CPS meets the appropriate Security Outcomes and Postures from the ONR SyAPs Annexes [30].

The development of the CPS (as part of the ISS) is discussed further in Section 32.8.

32.6.11 Assumptions and Commitments

No Assumption or Commitments are raised against a future Dutyholder / Licensee / Permit Holder with regard to cyber security at Version 3 of the E3S Case.

Other working assumptions made to allow the CSRA to progress are recorded in the relevant Tier 2 and Tier 3 documents and collated on the RAIDO Log [11] These assumptions will be checked and removed or managed as part of the continuing development of the Security Case. They will not necessarily become an assumption on future Dutyholder / Licensee / Permit Holder.

32.7 Vital Area Identification and Categorisation

32.7.1 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 32.7-1.

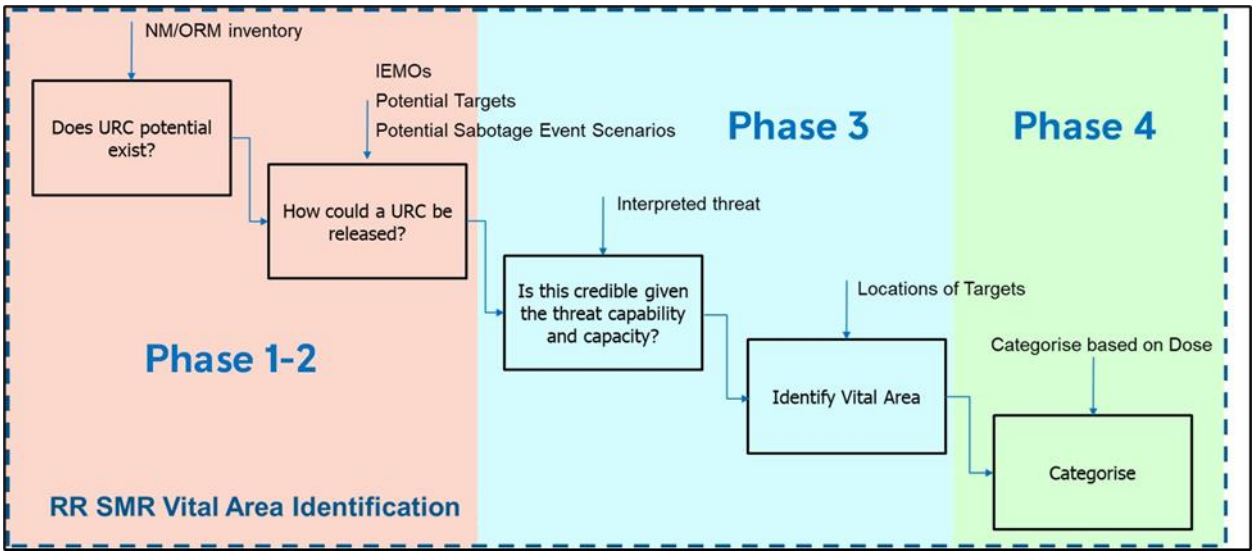


Figure 32.7-1: Vital Identification Process

A structured VAI&C methodology [7] has been developed in line with RGP (both international and UK national). This methodology identifies potential physical and cyber threats which could result in an URC.

32.7.2 Relevant Tier 2 and Tier 3 Evidence

This section of Chapter 32 summarises the CAE relevant to VAI&C.

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

- Rolls-Royce SMR: Vital Area Identification and Categorisation Methodology [48].
- Rolls-Royce SMR: Vital Area Identification and Categorisation Report [22].

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:

[Claim 32.4] The threat of sabotage of the Rolls-Royce SMR is minimised through the development of proportionate security measures as part of a Physical Protection System (PPS) which is included within an Integrated Security Solution (ISS).

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] The design basis threat of the sabotage of nuclear material or other radioactive material which could result in Unacceptable Radiological Consequence is 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.

[32.4.2] 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.

[32.4.3] 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.

[32.4.4] The security solutions to address the sabotage risk (from physical, cyber or blended attack) to the RR SMR design are developed and included with the Integrated Security Solution.

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

32.7.4 Vital Area - Definition

The glossary to the ONR SyAPs [17] defines a Vital Area as follows:

> 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.

Rolls-Royce SMR Ltd base the VAI&C for the RR SMR on the identification, as potential sabotage targets, of NM and ORM and the SSCs which contribute to the provision of the FSFs to that NM and ORM. As such, VAI&C is carried out with regard to such material and SSCs rather than against defined areas of the RR SMR. It should be noted that - systems providing FSFs are not necessarily located in a single area but are co-located across wider areas (for example the Nuclear Island). Following the analyses, the locations where sabotage targets are confirmed are identified for protection as Vital Areas.

An 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 unmitigated 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 [30]. 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 32.7-1. Areas containing NM/ORM where sabotage does not lead to an URC are still identified as they need security protection (against theft) as Baseline Areas.

Table 32.7-1: Categorisation of Vital Areas

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

The atmospheric dispersion of radioactive materials is an energetic process. This energy could originate from either the attack itself (e.g. through use of explosives) or as a release of energy from within the target (e.g. through release of heat and/or pressure). Depending on the target, this release of energy could result from direct and/or indirect attack.

32.7.5 Approach to VAI&C for the RR SMR

32.7.5.1 Introduction

As outlined above, an URC is defined against a radiological dose threshold. Hence the target of the sabotage attack should contain a sufficient amount of nuclear or other radiological material; and the attack should be capable of generating an airborne plume which results in an above threshold dose. Some nuclear or other radioactive material may be in a form that is readily dispersed; likewise, not all DBT threats will be sufficiently energetic to result in aerial dispersion.

The preliminary identification of targets on a RR SMR which could generate an URC can be defined as:

- Nuclear fuel.
- Radioactive wastes and other radioactive material.

VAI&C is undertaken for all operating modes of the RR SMR [1]. For practical purposes, power operations and shutdown modes (Modes 1 to 5B) [1] and refuelling modes (Modes 6a and 6B) [1] are considered separately. This is a reflection of the fact that SSCs providing FSFs differ significantly between these two sets of modes.

32.7.5.2 Potential Targets- Nuclear Fuel

Nuclear fuel is a potential target at any point along the fuel route [55] from receipt of new (unirradiated) fuel to the on-site storage of spent (irradiated) fuel in a dry cask store. The locations where fuel will be present are:

- In Containment:
  - fuel in reactor.
- In Spent Fuel Pool Area:

- New fuel.
- Spent fuel.

- In Cask Storage Area:
  - Spent fuel (in casks).

All of the above locations, NM and ORM and relevant SSCs within them, are candidates for VAI&C. In addition to these specific locations, fuel (both new and spent) is a potential target when transferring between these locations.

The risk profile of sabotage and theft changes when material is being moved. Vital Area assessment will specifically consider those scenarios that may impact nuclear material during movements both inside and outside the reactor island, including for example the receipt of fresh fuel and the transfer of spent fuel casks to the Cask Storage Area.

32.7.5.3 Potential Targets – Radioactive Waste and other Radioactive Materials

32.7.5.3.1 Introduction

The RR SMR will generate a range of both ILW and LLW [57]. As discussed with regard to CfT, the detailed characterisation of these wastes cannot be undertaken until such are generated during operation of the RR SMR. Nevertheless, as part of the E3S Case estimated volumes and indicative dose rates will be derived for the waste streams. This information supports a VAI&C for these wastes.

Discrete radioactive sources are also potential targets for sabotage.

Components and structures could become radioactive as a result of irradiation during the operation of the RR SMR. The physical form of these components and structures mitigate against an URC occurring as a result of a sabotage attack (for example, the DBT is not capable of creating sufficient atmospheric dispersion from solid metal objects). Nevertheless, such materials are not automatically excluded from consideration as targets.

32.7.5.3.2 Direct Attack

A direct attack is one in which the DBT threats are applied directly to target material or the immediate containment of such. For the majority of sabotage events identified, such attacks would require the application of highly energetic DBT threats to result in an URC.

32.7.5.3.3 Indirect Attack

For the purposes of VAI&C, an indirect attack is one in which the SSCs which provide FSFs are attacked, resulting in the release of energy from within the target and subsequent atmospheric dispersion. These FSFs are

- Control of Reactivity (CoR).
- Control of Fuel Temperature (CoFT).
- Confinement of Radioactive Material (CoRM).
- Control of Radiation Exposure (CoRE)[3] .

[3] CoRE refers to control of exposure to radiation (alpha, beta, gamma and neutrons) direct from an exposed source (for example, nuclear fuel). CoRE is provided through shielding measures; the compromise of shielding measure is not generally relevant to VAI&C which is concerned with the release and atmospheric dispersion of radioactive material rather than direct dose from an intact source.

For the RR SMR, the primary potential for indirect attacks is against the nuclear fuel within the RPV and stored within the Spent Fuel pool. The compromise of a FSF could result in fuel degradation, which if unmitigated could result (ultimately) in core melt and atmospheric release leading to an URC. For radioactive waste and any discrete radioactive sources, only a direct attack would potentially result in an URC; these targets do not typically contain sufficient energy to promote atmospheric dispersion.

To be successful, a sabotage attack would need to be able to compromise both the systems providing the relevant FSF during operation (often referred to as a duty system) and those systems providing the safety functions during faulted and accident conditions (namely safety measures). Information regarding the relevant duty and safety systems is obtained from the Safety Case [67] [68] and supporting Fault Schedule [69].

The Safety Case for the RR SMR is built around the provision of five levels of (safety) DiD, which are (with success criteria shown in brackets) [37]:

- (DiD 1) Duty Systems - which provide the FSFs during operation (no fuel failure).
- (DiD 2) Preventative Safety Measures - which seek to provide the FSFs by alternative means (no fuel failure).
- (DiD 3a and 3b) Protective Safety Measures - which seek to provide the FSFs by an alternative means if the preventive measures have failed to do so (3A [up to Passive Decay Heat Removal safety measure] no fuel failure: 3b [Emergency Core Cooling safety measure] only some fuel cladding failure, containment intact).
- (DiD 4) Mitigation Measures – which. in the event that the protective and preventative safety measures have failed to be fully effective in preventing core melt, seek to prevent release of radiological dose to beyond the immediate point of release (core melt is retained at the bottom of the RPV, containment intact).
- (DiD5) Emergency Response Measures – which come into effect if DID level 1 to 4 are not effective, that is radiological material has been released (fuel melt plus containment breached).

In order for an indirect sabotage attack to result in a URC, it would need to compromise all of the SSCs provided for DiD level 1 to 4. Such combinations of SSCs are termed as a Potential Sabotage Event Scenario (PSES); the order in which they are compromised is taken into account when assessing the credibility of the PSES and the capability of the threat to result in an URC.

Typically, Level 5 may not come into action until a radiological release has occurred and should not be relied upon to stop such a release progressing to an URC.

32.7.6 Overview of the VAI&C Methodology

32.7.6.1 Introduction

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

Figure 32.7-2 presents the overall VAI&C methodology stages from Preliminary Assumption-based Assessment (PAA) to Phase 4.

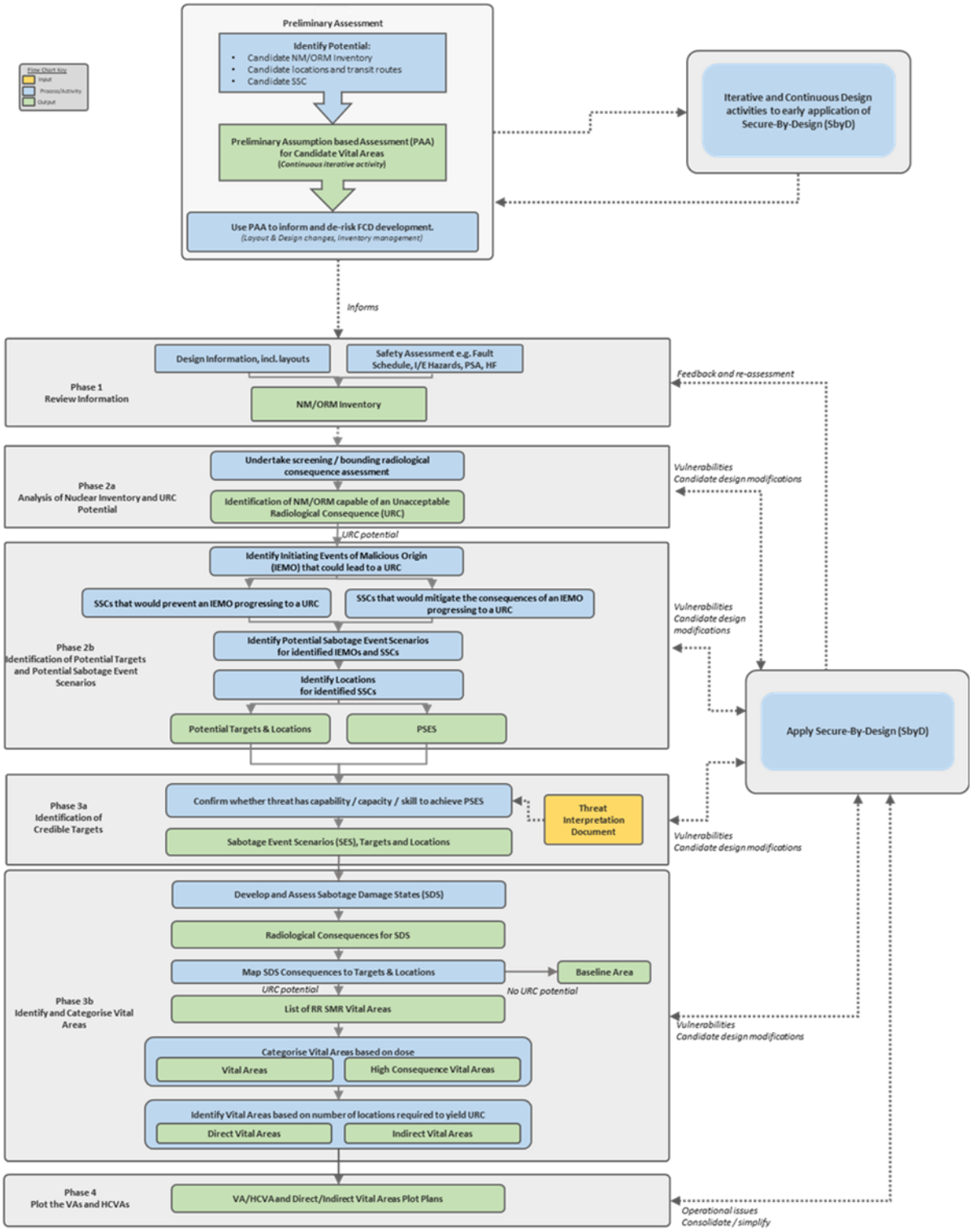


Figure 32.7-2: Overview of Vital Area Identification and Categorisation Methodology

32.7.6.2 Preliminary Assumption-based Assessment

The PAA 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 principles at a time where the ability to influence the design is arguably at its greatest.

The PAA is initiated after Stage 1, Step 1 of the SbyD methodology [38]. This includes the completion of an SbyD Initial Assessment by the work package owner (i.e. a design engineer) which is reviewed by a security Subject Matter Expert (SME) to determine the relevance to SbyD. Answering 'Yes' to any single question on the SbyD Initial Assessment qualifies the work package for further assessment i.e. the PAA.

In the PAA, SSCs requiring analysis as part of VAI&C are identified from the following information:

- Potential locations of safety systems or components which play a major role in maintaining the FSFs; the failure of which (alone or in combination) could potentially lead to any undesirable consequence pertaining to an URC.
- High-level known locations (including internal transit routes as applicable) of major sources of NM or ORM considered likely to have URC potential if sabotaged.
- Potential locations for control of the plant/process.
- Plant areas likely to be Vital Areas on a 'typical' Pressurised Water Reactor (PWR) from experience.

No formal assessments or calculations are made in the PAA. All assumptions, judgements and potential vulnerabilities identified (at a high-level) during the PAA are recorded.

32.7.6.3 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.

32.7.6.4 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 an 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 an 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 PSESs at this stage) are derived to inform subsequent phases of the assessment.

32.7.6.5 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.

Phase 3b outlines the final damaged state of the plant and an assessment of the radiological consequences of a release for each credible SES is undertaken, using data generated from appropriate Radiological Consequences Methodologies [70] [71]. Initially, data generated to support safety analysis is used; if this is not representative of a sabotage scenario consequence, security specific modelling will be undertaken.

Vital Areas are identified and categorised for the locations of each Target to support the subsequent development of potential security measures.

32.7.7 Outputs from VAI&C

The overall approach to VAI&C is based around: the provisional high-level identification of potential targets; and the FSFs the delivery of which need to be compromised for a sabotage attack to result in a URC; and an understanding of the SSCs which provide the (safety) DiD against the propagation of the analogous fault sequences.

As the VAI&C progresses, a set of SESs will be identified for each of the provisional targets (and any other identified during the process) for each of the FSFs relevant to these targets. These SES will include both direct and indirect attack and include blended attack threats [72].

The SSCs covered by the VAI&C analyses are identified as relevant through the PAA process. Each of the workshops covers a group of SSC linked around the FSF they provide and the target of interest.

VAI&C workshops are being held as the design of relevant SSC matures (typically reaching DR3 maturity). It should be noted that the workshops themselves are part of the overall SbyD approach and that this timing (in terms of DR maturity) supports the SbyD input into the design.

A consequence (of how the workshops are being delivered) is that the SSCs covered in an individual workshop do not necessarily cover all SSCs that would be included in the relevant fault sequences and, hence do not cover all the SSCs that are identified in PSESs. This is to be addressed by the collation of the outputs from the various workshops into an overall summary set of complete PSES.

Each workshop covers a grouping of systems, based around the delivery of one of the FSFs. The workshops are held in two parts:

- An initial stage (which covers Phase 1 and 2); and, in part stage 1 is undertaken prior to the workshop, with relevant fault sequences being identified and SSC design information reviewed by the Security Team prior to discussion about such at works as part of phase 2.
- A second workshops which covers (Phases 3 and 4). It is this latter part which makes use of the DBT, radiological consequence data and assesses the credibility of an attack.

The analysis in the workshops focuses on operational modes 1 to 5B, during which the plant operates in a controlled state. Refuelling modes (6A and 6B) are excluded from this scope as they present unique Examination, Maintenance, Inspection, and Testing (EMIT) activities and have increased system accessibility requirements that differ from normal operations. Modes 6A and 6B also entail

an increased presence of personnel, creating the potential for event scenarios distinct from those in power operations. Dedicated VAI&C analyses will be conducted separately to address the specific shutdown conditions related to the refuelling modes.

The workshop grouping analysed to date are:

- Reactivity Control Safety Measures, these are Safety Class 1 and 2 s SSCs which deliver the FSF of CoR to the nuclear fuel in the RPV [73].
- Reactor Coolant Systems, these are Safety Class 1 and 2 SSCs which deliver the FSF of CoFT to the nuclear fuel in the RPV [74].
- Steam and Feed Systems, these are Safety Class 1 and 2 SSCs which deliver the FSF of CoFT to the nuclear fuel in the RPV [75].
- Containment Systems, these are Safety Class 1 and 2 SSCs which deliver the FSF of CoRM to the nuclear fuel in the RPV [76].

The systems included in these groups are listed in the respective Tier 3 analysis reports.

For Phase 1 and 2, the analysis reports include details of:

- Any assumption made to facilitate a meaningful workshop (for example where relevant information).
- The identification of the relevant direct or indirect target inventory of NM and ORM; in the absence of relevant dose information, assumptions are made regarding the URC potential.
- The identification of IEMO (typically based on postulated initiating events (PIEs) identified in the faults schedule) and PSES.
- Candidate design modifications, which could potentially reduce security risk and, hence, reduce requirements for protective security measures.

The assumption made (including regarding URC potential) are to be confirmed or otherwise, once relevant information is available. These assumptions are entered onto the RAIDO Log [11].

For Phases 3 and 4, the analysis reports include details of:

- Credible target analysis against the DBT threat profile (including for blended physical and cyber attacks) whether the attack is direct or indirect.
- Radiological Consequence Analysis (as available).
- The plotting of vital areas.

The VAI&C analyses noted above have identified SSCs that are part of an SES which requires protective measures against a sabotage threat. This includes both complete systems and individual components within systems; an example of the latter are isolation valves.

The areas of the RR SMR in which these systems and components are located are plotted as Vital Areas within the Tier 3 analysis reports[4].

At the time of drafting this Tier 1 document, radiological consequences (Radcons) data to support the safety case have not yet derived (this is due for later in 2025). Hence such information is not, as yet, available to support the VAI&C analyses.

[4] The Tier 3 analysis report are classified as SNI:OS and hence further detail regarding these systems and component is not provided in this Tier 1 Chapter.

On this basis, the output from the analysis is the identification of Candidate Vital Areas, which are provisionally categorised as HCVAs. This provisional categorisation will be readdressed once Radcons data is available.

The provisional categorisation of vital areas will be readdressed as the assumptions made within the analyses are confirmed or otherwise, and to reflect any design changes (including potential SbyD modifications identified by the VAI&C workshops).

32.7.8 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 are assigned to security SSCs. This is undertaken as part of the overall SbyD Approach.

Prior to the availability of Radcons data, a conservate assumption is that the reactor island may include one or more high consequence vital areas. This assumption is made to allow for the concurrent development of the ISS; clarification on this assumption will be included in the up-issue of the Tier 2 VAI&C Report [22] and ISS Report [23] later in 2025.

32.7.9 Conclusions and Forward Look

The VAI&C identify the NM (and ORM) and SSCs, the sabotage of which could, if unmitigated lead to an URC. The VAIC is undertaken against a threat profile based on the UK DBT; this includes for both an insider threat and a blended attack.

In conjunction with the identification of sabotage targets, the VAI&C identifies requirements on engineering design and site layout (to reduce risk) and/or requirements for dedicated security measure to address the residual risk. These requirements are for security measures which deliver both physical security functions and cyber security functions. Security requirements are captured within the Rolls-Royce SMR Limited requirements management database [10].

VAI&C is an iterative process, the outputs from which should be reviewed in light of design changes or other relevant information becoming available. More specifically, any VAI&C analyses undertaken before Radcons data is available will be reviewed once this data is available.

Although dependent on the design maturity of SSCs, priority is given to analysis of the targets and SSCs associated with the main source of URC risk, the nuclear fuel within an operational reactor. On the basis of this prioritisation, the outline programme for VAI&C analyses is:

- Nuclear Fuel in Containment –
  - Complete Analysis by end of 2025 (caveated by dependencies and possible reviews).
- Nuclear Fuel in Spent Fuel Pool Area -
  - Identification of applicable safety case by end of 2025.
  - Start analysis process to complete in 2026.
- Radioactive Wastes and Other Radioactive Materials (including discrete sources) -
  - Identification of applicable safety case by end of 2025.
  - Analysis process planned for 2026.
- Cask Storage –
  - Identification of applicable safety case by end of 2025.
  - Pending final decision on technology and withstand against DBT.

  - Unlikely to be any detailed analysis by end of 2026.
- Impact of material movements on VAs –
  - Identification of applicable safety case by end of 2025.
  - Assumption based application to ISS.
  - Detailed analysis in association with site-specific design (i.e. post-GDA).

The output from VAI&C is taken forward into the ISS through the identification of the appropriate Security Outcomes and Postures from the ONR SyAPs [28]. These are taken forward into the ISS. In the absence of Radcons data, the design of the ISS is proceeding with a conservative assumption regarding potential HCVAs.

Outcomes and postures will be achieved through the provision of both physical and cyber security functions delivering and a Graded Approach and Defence-in-Depth.

The VAI&C for the RR SMR is on-going and will continue through to the end of GDA and beyond. The prioritisation of SSCs outlined above ensures that the source of NM which present the greatest security risks of area addressed during GDA.

On this basis, the ISS will deliver Security Outcomes and Postures which address the protection. of greatest risk sources and hence is conservative with regard to the lower risk sources. Furthermore, security risk associated with radioactive waste and cask storage will not be realised immediately on construction and operation of a RR SMR with facilities for storage only being constructed after several years of operation. This should be addressed by a relevant site specific VAI&C for these storage facilities.

32.7.10 Assumptions and Commitments

The following Assumption or Commitments are raised against a future Dutyholder / Licensee / Permit Holder with regard to VAI&C:

- [Commitment-32.4.0014] A future Dutyholder / Licensee / Permit Holder should review the VAI&C for the RR SMR site on a regular basis and when there are any significant changes to engineering design, the Safety Case, the ISS or the appropriate threat profile (DBT in the UK).
- [Commitment-32.4.0015] A future Dutyholder / Licensee / Permit Holder should undertake a site-specific VAI&C study for NM being moved onto/off and within a site's vital areas and ensure that the required Security Outcomes and Postures are met by the security measures in place for such.
- [Commitment-32.4.0057] A future Dutyholder / Licensee / Permit Holder should undertake a site-specific VAI&C study for waste and spent fuel storage facilities and ensure that the required Security Outcomes and Postures are met by the security measures in place for such.

Other working assumptions made to allow the VAI&C to progress are recorded in the relevant Tier 2 and Tier 3 documents and collated on the RAIDO Log [11]. These assumptions will be checked and removed or managed as part of the continuing development of the Security Case. They will not necessarily become an assumption on a future Dutyholder / Licensee / Permit Holder

32.8 Integrated Security Solution

32.8.1 Introduction

The SbyD approach (see Section 32.4) 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 provides 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 of 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, which is described in more detail in the Tier 2 ISS Report [23].

This approach 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.

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

Through 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.

32.8.2 Relevant Tier 2 and Tier 3 Evidence

This section of Chapter 32 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 [23].

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

32.8.3 Claims Addressed

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

[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 summarised in Section 32.17 (Appendix E).

Rolls-Royce SMR Limited recognises that the current claims structure of the ISS requires further rationalisation and development. This is being undertaken in conjunction with the development of the ISS.

32.8.4 Philosophy of ISS

Historically, nuclear security requirements for nuclear power stations were prescribed by the relevant regulatory authority. Over the last decade there has been a shift from a prescriptive approach to an outcome-focused model, giving more freedom in designing security solutions.

Subsequent to the issue of the ONR SyAPs [13], the regulatory regime for nuclear security in the UK has become more permissive. Dutyholders must now meet specific Security Outcomes and Postures, determined through security analyses assessing risks of sabotage, theft (of nuclear material and/or radioactive material), and cyber-attacks. Typically, these analyses were conducted on a final (or nearly complete) engineering design for a nuclear power station.

The resulting security solutions usually included a PPS and a CPS as ‘add-ons’ to the engineering design, not an inherent part of it. The PPS and CPS were integrated to the extent that there was physical protection of cyber systems.

As digital control systems become more prevalent and cyber threats more sophisticated, CPS requirements have grown, necessitating both cyber and physical protection. The increasing threat of blended attacks (combined physical and cyber-attacks) has driven the integration and convergence of PPS and CPS.

The Security by Design (SbyD) approach adopted for the RR SMR integrates the PPS and CPS from the initial design stages. This approach helps reduce security vulnerabilities, lessen the requirements for PPS and CPS, and increase resilience.

The goal is to develop a truly integrated solution where security is embedded into the design and future operation of the RR SMR. An important aspect of the RR SMR ISS is its construction, which

allows tracking of measures, assumptions, and risks from the security plan through the ISS, PPS/CPS, and analysis, ultimately linking back to design decisions.

32.8.5 Approach to the Development of the ISS

32.8.5.1 Scope of ISS

The following security analyses are applied to the RR SMR design to identify potential vulnerabilities and areas for inherent security improvements:

- Categorisation for Theft (see Section 32.5).
- Cyber Security Risk Assessment (see Section 32.6).
- Vital Area Identification & Categorisation (see Section 32.7).

The Integrated Security Solution (ISS) demonstrates how the relevant Regulatory Outcomes are met within the RR SMR generic design. These Regulatory Outcomes focus on

- Preventing the significant off-site release of radioactivity.
- Preventing the theft of NM or ORM.
- The compromise of SNI.

These outcomes, along with associated postures, are achieved through the designation of security functional requirements and the design of the Structures, Systems, and Components (SSCs) that provide these functions. The achievement of these outcomes is recorded in the requirements management system.

Regulatory Outcomes are not included within Chapter 32 itself. They will be presented in the relevant Tier 2 reports and supporting Tier 3 documents (which will be classified as SNI)

While security measures that protect against significant off-site release also safeguard the commercial operation of an RR SMR, additional measures may be taken to enhance economic resilience.

32.8.5.2 Integration

The ISS integrates physical and cyber protection measures to ensure they work cohesively. The development of the ISS is aligned with the SbyD approach and engineering design, contributing to the overall integrated E3S solution that delivers the fundamental E3S objective for the RR SMR. The ISS includes:

- 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) and delay (for example security doors).

32.8.5.3 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 [27], 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 National Protective Security Agency (NPSA), via their extranet, from their Quarterly Threat Reports, Cyber Assurance of Physical Security Systems [77], Operational Requirements guidance [78] 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 [79] 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 [80] 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.

32.8.5.4 Security Analyses

As outlined earlier, Rolls-Royce SMR Limited has developed methodologies to assess the inherent security of the generic design through analyses for VAI&C, CfT, and CSRA. The goal of these methodologies is to identify sensitive SSCs that require protection by the ISS. SSCs include physical systems, digital systems, and software.

These methodologies are applied iteratively as the engineering design matures, allowing security concerns to influence the design. Vulnerability assessments will ultimately demonstrate whether the design solution, including inherent security features, achieves the necessary outcomes. Detailed analyses are conducted once the SSC design is sufficiently mature. Up to this point, SSC design is essentially optioneering, and the influence of security requirements is recorded as part of this process.

Detailed analyses identify the required outcomes that the ISS must meet in terms of protecting NM, ORM, SNI, and sensitive SSCs. These outcomes take into account any security benefits inherent in the design or resulting modifications identified by preliminary assessments.

The iterative development of the ISS aims to identify further design modifications that help eliminate vulnerabilities and achieve the required outcomes.

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

Equally, for design changes for reasons other than security, the Security Case Team are advised and comment on such [50]:

- Where these changes are beneficial to security, due credit is taken within the ISS.
- Where changes have a negative impact on security, these are discussed and recorded; 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 [53].

32.8.5.5 Delivering for the future Dutyholder / Licensee / Permit Holder

The ISS provides a future a future Dutyholder / Licensee / Permit Holder with:

- An understanding of how the 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 Dutyholder / Licensee / Permit Holder owned risks to be addressed as part of its implementation.

The ISS includes not only the security infrastructure provided by the PPS and CPS, but also the security benefits inherent in the wider engineering design.

Understanding these security benefits is crucial for future operators, who must review the security implications of altering the design or operation of relevant SSCs. This understanding would be lacking if the ISS relied solely on the PPS and CPS.

Due to the generic nature of the RR SMR design, assumptions are made about the commercial risk appetite of a future Dutyholder / Licensee / Permit Holder and how they will manage the site. These assumptions are recorded as part of the ISS.

Based on the plant design, security analysis, and assumptions about risk appetite and operations, Security Technical Specifications (Security Tech Specs) are produced and documented in the ISS.

Given the generic nature of the RR SMR design, some aspects cannot be fully addressed without site-specific details. Additionally, future technological developments in protective measures, changes in threats or regulations, or design changes from other E3S subject areas may necessitate recommended changes and alterations throughout the lifecycle. While assumptions can be made about the nature of a site and future technology changes, there remains a risk that redesign may be necessary.

32.8.5.6 Maturity of Design

The scope and detail in the ISS evolve with the engineering design of the RR SMR and as security analyses are completed.

A ‘generic’ ISS comprises the following:

- Confirmation of 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 computer-based systems.
- 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 a 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.

32.8.6 Concept and Requirements Development of for the ISS

32.8.6.1 Preliminary Concepts

The ISS is being developed against a maturing engineering design and layout and as security analyses are being progressed. To facilitate this approach, a high-level conceptual basis for the ISS is developed based on past experience and RGP.

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 those 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).

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 Tier 2 Report [23]. At a high level, this concept provides an indication of potential security zones and the associated protective measures (PPS and CPS) that could be included in a more mature ISS.

32.8.6.2 ISS Requirements

This conceptual basis drives the identification of security requirements to be delivered by 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 [51].

Company Standard Security and Safeguards Requirements and Analysis [78] describes 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 current threat interpretation [40]. 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. The ISS is designed in such a way that it can be adjusted to reflect changes to site specific design or threat (for example, in the UK the sector Threat and Government Response levels).

32.8.6.3 Concept for the Physical Protection System

32.8.6.3.1 Introduction

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 [37]. The PPS also considers business security risks. Further to this, the PPS also considers protection of computer-based systems.

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 computer based systems) 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.

32.8.6.3.2 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 [35], 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 32.2.4.

The ONR TAGs on Functional Categorisation and Classification [81], Policing [82], the Civil Nuclear Constabulary [83] and the Use of Civilian Guard Forces [84] allow Rolls-Royce SMR Limited to understand the regulator's expectations in these areas.

The Security Function Categorisation & Classification methodology [43] 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 [43] complements the more general E3S categorisation and classification methodology [41].

32.8.6.3.3 Physical Security Infrastructure

An indicative set of the security measures that comprise a typical PPS are provided in the ISS Tier 2 document [23], which also gives an indication of the security function delivered by these measures.

32.8.6.3.4 Physical Security Zoning

This sub-section sets 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.

A preliminary identification of potential security layers or 'zones' outside the Reactor Island is provided in Figure 32.8-1.

A final decision on the outer RR SMR boundary has yet to be made (and will be strongly influenced by site-specific considerations). The security concept for this boundary includes:

- 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 the Reactor Island.
- The hazard shield; from a radiation protection perspective and a likely dividing line for National Security Vetting (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).

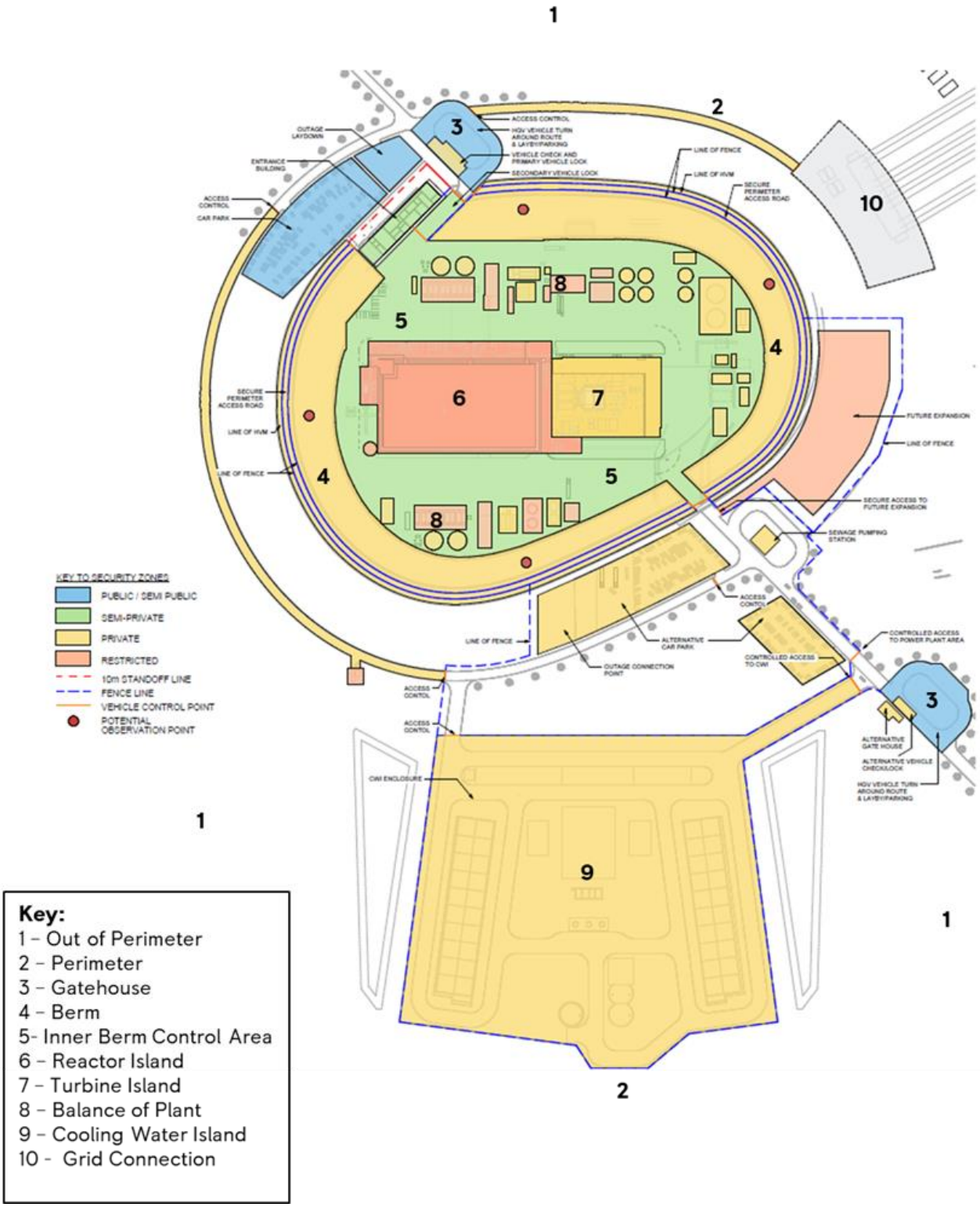


Figure 32.8-1: Concept for PPS Security Zones

32.8.6.3.5 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-actions. These include as follows [23]:

- Power & Space: Initial discussion on location and space requirements for the Security Control Centre (SyCC), and Emergency Control Centre (ECC), have been undertaken. Power requirements have yet to be defined. Power and space are also be required for the civil guard force and any on-site armed response force; this also includes provision of back-up power in the event of loss of grid power.
- Assumptions: During the development of security measures, assumptions are made (and recorded in the RAIDO Log) 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, RGP and previous OPEX.
- Human Based Security Claims: Human Factors (HF) applies knowledge of human characteristics to optimise the design of products, equipment, environments, systems [7].
- 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 future Dutyholder / Licensee / Permit Holder would also be operating outside the Security Case (in the UK the NSSP). Rolls-Royce SMR Limited will develop aspects of operations that are required for security measures, based on legal requirements, RGP and the derivation of assumptions. These operational aspects are designated as Security Tech Specs within the Security Case.

32.8.6.4 Concept for the Cyber Protection System

32.8.6.4.1 Introduction

Primarily, the CPS protects against cyber attack against computer-based systems, 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 that should be protected by the CPS.
- The Security Outcome to be delivered by the CPS, 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.

32.8.6.4.2 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 [10], which provides traceability from these functional requirements to the finalised security solution. Typical security functions are introduced in Sub-section 32.2.4.

The Security Function Categorisation & Classification methodology [43] 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 32.4.8.

The Functional Security Categorisation and Classification Methodology [43] complements the more general E3S categorisation and classification methodology [41].

32.8.6.4.3 Cyber Security Infrastructure

The relevant standards [62] [85] [86] identify controls that are either mandatory or optional depending on the system security degree and lifecycle phase.

IEC62645 [62] is the main standard used to generate the baseline and security degree requirements. This is augmented by IEC62443-3-3 [85] which provides additional technical requirements. As IEC62443-3-3 uses "security levels" rather than security degrees the requirements are mapped to the security degrees.

32.8.7 Development of the ISS

32.8.7.1 Development of the ISS - Physical Protection System

32.8.7.1.1 Introduction

This sub-section provides an overview of the development of the ISS for this version of the E3S Case The development of the PPS covers:

- The identification of assets requiring protection (including NM and associated protective or mitigating SSCs).
- Operational Requirements.
- PPS Outcomes Postures and Response.
- Site Zoning.

32.8.7.1.2 Identification of Assets Requiring Protection

Work has commenced on identifying assets below the zonal level across the design in order to inform target identification and support detailed PPS design. To date, individual physical assets, which include capabilities (such as power supply) to individual facilities (i.e. workshops, gas storage areas), are identified for future prioritisation and triage.

Once there is sufficient depth of analysis from VAI&C, CfT, vulnerability assessment and adversary pathway sequencing, assets will be reviewed to identify those that are exposed on a pathway for further treatment.

32.8.7.1.3 Operational Requirements

Development of the PPS has established a series of high-level protection objectives and operational requirements with the intent of codifying security requirements to achieve the designated security effect.

These security requirements are expressed as a set of Operational Requirements (ORs), which are being developed in a tiered fashion [78], as follows:

- Level 1 Operational Requirements: Level 1 establishes the required functional security effect to be achieved and proffer potential security solutions (for example, '*the boundary wall shall DELAY an attacker*').
- Level 2 Operational Requirements: Level 2 adds depth and additional specificity to the Level 1 OR and its functionality and may introduce specification standards (for example,

'*the asset shall DELAY an adversary engaged in a manual forced entry attack, in order to gain unauthorised entry*').

- Level 3 Operational Requirements: Level 3 defines performance criteria against the Operational Requirement (for example, *The asset shall withstand a Manual Forced Entry attack by an Enhanced attacker for a period of x minutes*').

This tiered approach to the development of ORs allows for effective shaping of design and layout and its scalable specificity allows for review through the design cycle and beyond into operation of a RR SMR.

ORs are indexed against threat capabilities and security risk to enable a future operator to revise, enhance or (where appropriate) relax the security controls in response to changing security postures. A baseline set of Level 1 ORs has been developed, with an indicative set of Level 2 ORs [87].

32.8.7.1.4 PPS Outcomes, Postures and Response

The PPS Outcome, Posture and Response (OP&R) for the RR SMR, including those to mitigate credible threats and vulnerabilities, are informed by the CfT and VAI&C analyses and align with the SyAPs Annexes [30]. This includes the outcomes, postures and response and the outcomes for the overall site and proposed security zones.

The required OP&R are being identified as the CfT and VAIC analyses proceed; and will be collated in a future supporting Tier 3 document[5].

32.8.7.1.5 PPS Security Zoning

A preliminary PPS zoning has been developed (see Figure 32.8-1). Zoning of the site delivers a wide variety of security benefits pursuant to establishing sufficient defence in depth.

PPS zoning also takes into account the 'operational' boundaries associated with the division of a RR SMR site into islands (for example the Reactor Island and Turbine Island) and the internal physical boundaries within these islands.

The principles of proportionality and a graded approach will be applied to any area segregation work. The intent being to ensure the appropriate level of security whilst enabling effective plant operations.

In future versions of this Chapter, this sub-section will set out more detail of the Security Zoning around which the PPS is based (with reference as appropriate to more detailed sources of evidence).

32.8.7.2 Development of the ISIS - Cyber Protection System

32.8.7.2.1 Introduction

The CPS protects Computer-Based Systems from malicious interference that could enable: the theft of NM or ORM; or the theft or compromise of SNI; and/or, the sabotage of either nuclear material or SSCs (which could result in an URC).

As a secondary goal, the CPS also protects Computer-Based Systems from malicious interference that could enable: the disruption business activities; the loss or disruption to the capability to generate power; the theft or compromise of sensitive business information; damage to property and environment; or harm to staff or the general public.

[5] This Tier 3 document will be classified at SNI:O-S

Based on threat interpretation (Reference [42]), and it should also consider business risks. These requirements for protection the cyber protection system will be identified from Threat Intelligence relevant best practices and the following security analyses.

32.8.7.2.2 CPS - Security Infrastructure

For every Computer-Based system within the scope of the RR SMR design, there will be a set of baseline security requirements. These baseline requirements are aimed at protecting systems from basic low skill cyber-attacks. The security degrees then layer on requirement enhancements and additional requirements to apply a graded approach to system protection.

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 [23].

Additional requirements have also been drafted to cover gaps in the standards based on RGP and operational experience. In the future, additional requirements will be drafted to ensure that systems are capable of integration with CPS provided security systems

During the design of computer-based systems, the consequence-based risk assessment methodology focuses on determining if the DBT can successfully cause high consequence events, However, the DBT only represents a theoretical threat. Designing to the DBT sets a high standard for the design of the security systems, and provides necessary stability to formalise requirements during design, but may not capture sudden changes to real world threat actor capabilities.

Once Computer-Based systems reach full design maturity, it will be very difficult to make further changes to the design. If new threat capabilities are developed/discovered after this point, the security team will need to provide a solid justification that the design needs to change.

Therefore, there is a need for a methodology that will test if real world threat actors could undermine the security case, and provide the evidence required to justify to all stakeholders that changes are necessary and proportionate. This methodology will be developed as part of the Cyber Security Performance Evaluation Specification.

32.8.8 Conclusions and Forward Look

The ISS protects nuclear material and other radioactive material (NM and ORM), safety critical SSCs and SNI against theft and sabotage; and RR SMR as whole against threats to commercial operations.

The ISS is a combination of security measures which achieve the required Security Outcomes and Postures [30] through delivery of appropriate security functions. This results in a multi layered security regime (Defence in Depth) which is proportionate to the risks (Graded Approach).

The ISS identifies the nuclear material and SSCs that require protection and the locations of such. This protection is a combination of both a physical protection system (PPS) and a Cyber Protection System (CPS); much of the ISS comprises physical security SSCs controlled by a digital computer-based operating system.

The ISS is being developed in tandem with both a maturing engineering design and layout and as security analyses are in progress; rather than following the completion of the design and subsequent identification of security risk.

To allow this parallel approach to proceed, professional judgement, together with reasonable assumptions, are used to develop a conceptual basis for the ISS based around past experience and knowledge of security regimes on other nuclear sites.

As the engineering design and layout mature and the security analyses are undertaken, the judgements and assumptions can be confirmed (or otherwise) and the design of the ISS becomes more detailed. For example, the ISS will require security cameras and access control; as the development of the ISS progresses, the number type and locations for such will be d determined and finalised.

This approach is iterative and is part of the overall SbyD approach. At times, it may be necessary to revisit and review parts work and update such on the basis of new emerging information.

Development throughout the next phase is primarily focused on articulating the security posture and future security regimen of the generic RR SMR plant. The priority will be to establish the baseline measures for both the PPS and CPS and developing an integration and convergence framework, in order to achieve the required security outcomes in a holistic manner. Additional table-top testing and wargaming will be used to validate assumptions and security measures that are in development.

Table 32.8-1 and Table 32.8-2 set out the Tier 3 documents that will support and inform the development of the ISS through Versions 4 and 5 of the E3S Case The output from this work will be summarised in future versions of this Chapter.

Table 32.8-1: Development of the ISS for Version 4 of the E3S Case[6]

E3S Case Tier	Document Title	Brief Description of Contents
3	Rolls-Royce SMR: Cyber Security Design Requirements Specification	The list of system level security requirements that will be assigned via the security degrees
3	Cyber Protection System Definition Document	The CPS Definition document lays out the overall strategy for the delivery of cyber security within the NPS design
3	Rolls-Royce SMR: Physical Protection System, Employment Strategies (various documents)	Series of strategy documents, articulating the employment of PPS elements, at a conceptual level. To include, but not limited to: access control, lighting, barriers, vehicular control and civil guard force
3	Rolls-Royce SMR: Physical Protection System, Nuclear Material Inventory Protective Strategy	Conceptual strategy outlining the physical security requirements for the protection of NM throughout the generic design, and how it integrates with wider security elements
3	Rolls-Royce SMR: System Outline Description (SOD) for the Integrated Security Solution	Describes the ISS at Initial Concept Design
3	Rolls-Royce SMR: Summary of Physical Protection System (Issue 1)	Physical Protection System: Initial design, PSMs, desired cause and effects, operational requirements, layout and assumptions. Incorporation of analysis informed decisions, security zones, application of

E3S Case Tier	Document Title	Brief Description of Contents
		graded approach (zonal mapping), diversification and Defence in Depth
3	Rolls-Royce SMR: Physical Protection System, Vital Area Protective Strategy	Conceptual strategy on how the PPS will be configured to protect Vital Areas, identify protective security postures (SyAPs) and detail mitigations

The Tier 2 and 3 documents included on Table 32.8-1 will be available for assessment during GDA, prior to incorporation in the Tier 1 Chapter as part of Version 4 of the E3S Case.

Table 32.8-2: Development of the ISS for Version 5 of the E3S Case

E3S Case Tier	Document Title	Brief Description of Contents
3	Cyber Protection System Performance Evaluation Specification	Document detailing the testing, evaluation, and auditing activities of the security of the SMR design, throughout the lifecycle of the power station
3	Rolls-Royce SMR: Physical Protection System, Vital Area Protective Strategy	Conceptual strategy on how the PPS will be configured to protect Vital Areas, identify protective security postures (SyAPs) and detail mitigations
3	Rolls-Royce SMR: Physical Protection System, Initial Site Operational Phase Review	Initial impact analysis on the PPS throughout the sites different operational phases and identifies any potential variations in posture and configuration required to support transition and/or sustainment between operational phases
3	Rolls-Royce SMR: Summary of Physical Protection System	Physical Protection System: Updated design, PSMs, desired cause and effects, operational requirements, layout and assumptions. Incorporation of analysis informed decisions, security zones, application of graded approach (zonal mapping), diversification and Defence in Depth
3	Rolls-Royce SMR: Security Measure Design Description for the Integrated Security Solution	Describes the ISS at Full/Final Concept Design
3	PPS Testing & Modelling Report	Report on testing, modelling & validation of the PPS against the DBT and Threat Scenarios
3	Rolls-Royce SMR: Summary of Physical Protection System	Physical Protection System: Initial design, PSMs, desired cause and effects, operational requirements, layout and assumptions. Incorporation of analysis informed decisions, security zones, application of graded approach (zonal mapping), diversification and DiD

E3S Case Tier	Document Title	Brief Description of Contents
3	Rolls-Royce SMR: Physical Protection System, Zonal Protective Design (various documents)	Series of design reports, drawings and operational requirements on ensuring the PPS supports the effective compartmentalisation of the generic site into security zones, detailing their individual characteristics, security effects to be achieved and interdependencies, redundancies & any risks that will require further development in licensing
3	Site Operational Review	Detailed impact analysis of on the PPS throughout the sites different operational phases and identifies any potential variations in posture and configuration required to support transition and/or sustainment between operational phases

The Tier 2 and 3 documents included on Table 32.8-2 will not be available for assessment during GDA. They will be incorporated in the Tier 1 Chapter as part of Version 5 of the E3S Case.

The scope of work outlined in Table 32.8-1 and Table 32.8-2 does not cover the entirety of the work required to develop the ISS which will continue beyond Version 5 (again in conjunction with a still maturing engineering design and layout). This will involve not only the ISS for the generic design but also site specific adaptions.

Future development of the ISS will comprise work that includes (but is not be limited to):

- Vulnerability Assessment to test the security measures and validate that they can achieve the required outcomes. When effectively applied, a vulnerability assessment can determine weakness in a system to allow redesign to take place or additional security measures to be developed. An initial vulnerability assessment will be undertaken when the OSS is at a sufficient maturity.
- Adversary Pathway/Sequence Modelling is a critical tool in designing security measures for nuclear security. This methodology involves analysing potential routes and methods that adversaries might use to breach the facility's defences. By identifying these pathways, we can evaluate the effectiveness of the planned measures and identify any additional vulnerabilities.

Further details of the development of the ISS post Version 3 of the E3S Case are set out in the ISS Tier 2 document [23].

It is expected that the ISS will continue to be updated throughout the lifetime of the RR SMR to take into to account general engineering development, site-specific learning and changes to threat profile and capabilities.

32.8.9 Assumptions and Commitments

No Assumption or Commitments are raised against a future Dutyholder / Licensee / Permit Holder with specifically with regard to ISS at Version 3 of the E3S Case. Assumptions raised with regard to other sections of this Chapter are relevant (see Table 32.11-1).

Other working assumptions made to allow the development of the ISS to progress are recorded in the relevant Tier 2 and Tier 3 documents and collated on the RAIDO Log [11]. These assumptions will

be checked and removed or managed as part of the continuing development of security case. They will not necessarily become an assumption on future Dutyholder / Licensee / Permit Holder.

32.9 Integration of Security with Other Topic Areas

32.9.1 Introduction

The Security Case forms part of the Integrated E3S Case; there are 33 chapters in total. Chapter 32 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.

32.9.2 Relevant Nuclear Security Claims

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

[E3S Claim 32.1] 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:

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

[32.1.4] Security measures have been integrated into SSCs in a way that is consistent with the operational intent of the Rolls-Royce SMR.

[32.1.4.2] Definitions for SSCs incorporating security functionality have been validated to demonstrate that the security measure has been achieved.

[32.1.4.3] Roll-Royce SMR key performance criteria have not been unduly impacted by the security functionality.

[32.1.5.1] Proposed security measures 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.

32.9.3 Forward Look

Table 32.18-1 in Section 32.18 (Appendix F) 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. The arguments and evidence for the substantiation of the above claims is presented in the Sections of this chapter covering the SbyD and the ISS and in the supporting Tier 2 documents to these topic areas.

32.10 Development of a Site Security Plan

32.10.1 Introduction

The primary objective of the ISS is to provide a future Dutyholder / Licensee / 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 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 transition 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.

In order to aid the transition to a NSSP (in the UK), the ISS will be mapped against the expectations within the ONR SyAPs [17]. A similar approach would be taken for any international deployment of a RR SMR.

32.10.2 Relevant Tier 2 and Tier 3 Evidence

This section of Chapter 32 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 [23].

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

32.10.3 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 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 Section 32.17 (Appendix E).

32.10.4 Site Licensing - Lifecycle Considerations

32.10.4.1 Licensing

Once a site has been selected, site licensing activities start. Part of this is the production of a site security plan, along with relevant supporting arrangements, and a separate security contingency plan (SCP). The site security 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.

32.10.4.2 Responsibility for Security Plan Production

It is the responsibility of a future Dutyholder / Licensee / Permit Holder to produce security plans for all phases of a facility lifecycle, in accordance with relevant legal and regulatory requirements.

The Security Case, specifically the ISS, provides the information to form the basis of these plans, appropriately tailored for and added to by site-specific information.

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

32.10.4.3 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 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 Preparedness and Response (EP&R).

32.10.4.4 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.

32.10.4.5 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.

32.10.4.6 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.

32.10.5 Security Tech Specs

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

32.10.6 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 security measures are tested:

- For the PPS this may include what emergency arrangements need to be available, such as an emergency control centre, and how this interacts with the security control centre, as included in the control facility description document [86].
- 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 DBT.
- Specifically for the CPS this should include such methods as penetration testing to assess for both malicious attack and accidental leakage or misuse.

Site specific designs for a RR SMR might also include for an off-site emergency control centre (ECC). This would allow a coordinated response (in the event of unavailability of the CC), across all disciplines, such as safety, environment, security (including physical & cyber), and the blue light services, to all incidents.

As part of the deployment of a fleet of RR SMRs, consideration could also to be given to the provision of a Cyber–Security Operations Centre, to ensure adequate resource is available to tackle cyber-attacks and facilitate recovery afterwards. This is not the current intention for a generic single site unit.

The ONR has published relevant TAGs [88] [89] [90]. These TAGs enable Rolls-Royce SMR Limited to understand the regulators expectations in these areas.

32.10.7 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 the ISS, to allow subsequent inclusion in a CSSP and NSSP.

32.10.8 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 [17]. 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.

32.10.9 Non-UK Regulatory Regimes

The CPPNM [24] 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 [27], and the rest of the IAEA Security Series. Nation States adapt the obligations and IAEA guidance into legislative requirements 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.

32.10.10 Conclusions and Forward Look

Alignment with the regulatory requirements for a UK NSSP is reviewed at appropriates points in the development of the ISS. This will include a gap analysis against the expectations of the ONR SyAPs.

Further details will be included in future version of this Chapter.

32.10.11 Assumptions and Commitments

Assumption or Commitments raised against a future Dutyholder / Licensee / Permit Holder are outlined in other sub-sections of the chapter and summarised in Table 32.11-1.

No Assumptions or Commitments are raised specifically with regard to this Section at Version 3 of the E3S Case.

32.11 Conclusions

32.11.1 Secure by Design

This Chapter outlines development of a 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 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 developed at Version 3 of the E3S Case. The Security Case (as part of the E3S Case) is being developed alongside the on-going 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.

32.11.2 Assumptions and Commitments on Future Dutyholder / Licensee / Permit Holder

32.11.2.1 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 [90].

32.11.2.2 Security Case

The Assumptions and Commitments raised on a future Dutyholder / Licensee / Permit Holder for the security case, ay Version 3 of the E3S Case, are as presented in Table 32.11-1.

Table 32.11-1: Assumptions and Commitments on Future Dutyholder / Licensee / Permit Holder

Assumption/Commitment	ID[7]	Description
Commitment	32.2.0003	A future Dutyholder / Licensee / Permit Holder should identify and characterise all ILW/LLW as it is generated to facilitate accurate categorisation for theft.
Commitment	32.2.0004	A future Dutyholder / Licensee / Permit Holder should identify and characterise all ORM that is generated to enable appropriate categorisation for theft.
Commitment	32.4.0014	A future Dutyholder / Licensee / Permit Holder should review the VAI&C for the RR SMR site on a regular basis and when there are any significant changes to engineering design, the Safety Case, the ISS or the appropriate threat profile (DBT in the UK)
Commitment	32.04.0015	A future Dutyholder / Licensee / Permit Holder should undertake a site-specific VAI&C study for NM being moved onto/off and within a site and ensure that the required Security Outcomes and Postures are met by the security measures in place for such
Commitment	32.4.0057	A future Dutyholder / Licensee / Permit Holder should undertake a site-specific VAI&C study for waste and spent fuel storage facilities and ensure that the required Security Outcomes and Postures are met by the security measures in place for such.

Working assumption have been made to allow security analyses and the development of the ISS to proceed; these are also captured in the RAIDO Log [11]. As additional information becomes available, the validity of the assumptions is confirmed or otherwise. Working Assumptions that are not validated will be passed onto to the future Dutyholder / Licensee / Permit Holder as Assumptions.

32.11.3 Conclusions and Forward Look

The generic E3S Case objective at Version 3 is

- Version 3 of the E3S Case shall provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective 'to protect people and environment from harm' as it is developed through detailed design. The case shall demonstrate that risks are capable of being reduced to as low as reasonably practicable (ALARP), using best available techniques (BAT), will be secure/safeguarded by design, and demonstrate sustainability for current and future generations.

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:

[7] These IDs are referenced against ID nos. generated in the RAIDO Log; as this numbering includes assumptions that might not be ultimately passed on to A future Dutyholder / Licensee / Permit Holder, Table 32.11-1 will not contain consecutive numbers.

The design of the RR SMR protects 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 Fundamental Nuclear Security Claim is decomposed into set of sub-claims (see Section 32.1.3), based on the five themes around which the Security Case is structured:

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

The arguments and evidence presented to meet the generic E3S Case objective at Version 3 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.

In conjunction with detailed security analyses (VAI&C, CfT & CSRA), the SbyD design approach has used the SbyD Principles 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.

This Chapter demonstrates that the framework for SbyD and the security analyses has been developed and how it is implemented as the security analyses are undertaken. This leads to the generation of security requirements (and security functions) which are either assigned to engineering design or layout SSCs or carried forward into the ISS for delivery.

The output from the security analysis (which are iterative in nature) are requirements on engineering design and site layout (to reduce risk) and/or requirements on the ISS for dedicated security measures to address the residual risk. These requirements are for security measures which deliver both physical security functions and cyber security functions. Security requirements are captured within the Rolls-Royce SMR Limited requirements management database [10].

The security analyses are on-going, with priority being given to analysis of SSCs associated with areas of the RR SMR which present greatest security risk (for example the Nuclear Island). Conservative assumptions are made to allow the analyses to proceed where the engineering design or safety case is not sufficiently mature or where relevant data is not yet available.

For example, in the absence of Radcons data, a working assumption for the design of the ISS is that there will be HCVAs associated with the Nuclear Island; as Radiation Consequences data becomes available, this assumption will be reviewed and the updated VAI&C in Version 4 of the E3S Case (and subsequent versions).

Prioritisations ensures that the most significant security risks are identified, initially in Tier 2 and 3 documents and subsequently in the Tier 1 document for Version 4 of the E3S Case. This gives confidence that the Security Outcomes and Postures [30] identified during GDA are a realistic representative of those that will be required for an operational RR SMR.

This version of Chapter 32 does not provide details of required Security Outcomes and Postures. These are being identified from the output from security analyses bit have not yet been formally

documented. Further details will be provided in the next (future) issue of the ISS Report [23] and supporting Tier 3[8] documents.

The ISS protects nuclear material and other radioactive material (NM and ORM), safety critical SSCs and SNI against theft and sabotage; and RR SMR as whole against threats to commercial operations.

The ISS is being developed alongside the on-going security analyses rather than on completion of such. To allow this to happen, a conceptual basis for the ISS has been developed based on experience, good practice and conservative assumptions regarding the security risk and Outcomes and Postures that are being identified as the analysis are undertaken.

The ISS identifies the nuclear material and SSCs that require protection and the locations of such; this includes Categorization of theft and the identification and categorisation of Vital Areas. This protection is a combination of both a physical protection system (PPS) and a Cyber Protection System (CPS); much of the ISS comprises physical security SSCs controlled by a digital computer-based operating system.

This protection is delivered through a combination of security measures which deliver the required security function in accordance with the Secure by Design principles, including Defence in Depth and the Graded Approach. This includes the protection of vital areas and other locations containing assets requiring protection.

Version 3 of this chapter is based primarily around the information presented in the Tier 2 and Tier3 document issued prior to drafting this chapter. The relevant issue of the ISS Report [19]. This issue (Issue 2, dated March 2025) essentially presents a high-level concept and a narrative about how this will be developed; this is reflection in Section 32.8.

The development of the ISS is on-going and will be presented in Issue 3 due for issue in December 2025. This issue will provide a greater level of detail, including more defined security boundaries and the scope and location of security measures. It will not present the detailed design and specification of security measures; this will not be achieved prior to completion of GDA.

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 [23] and supporting Tier 3 (see Table 32.8-1 and Table 32.8-2).

Issue 3 of the Tier 2 ISS Report will provide sufficient confidence that the ISS once fully developed will be compliant with NISR [16] and will deliver the Security Outcomes and Postures [30] appropriate to an operational RR SMR.

Further arguments and evidence to underpin claims will be developed in line with the E3S Case Route Map [2] 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.

[8] These Tier 3 documents will be classified as SNI.

32.12 References

[1] Rolls-Royce SMR Limited, SMR0004294, Issue 4, “Environment, Safety, Security & Safeguards Case Version 3, Tier 1, Chapter 1: Introduction,” August 2025.

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

[3] Rolls-Royce SMR Limited, SMR0004589, Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs,” August 2025.

[4] Rolls-Royce SMR Limited, SMR0003929, Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 7: Instrumentation and Control,” August 2025.

[5] Rolls-Royce SMR Limited, SMR0004010, Issue 4, Generic Environment, Safety, Security and Safeguards Case, Version 3, Tier 1, Chapter 8: Electrical Power, August 2025.

[6] Rolls-Royce SMR Limited, SMR0003778, Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 9B: Civil Engineering Works and Structures,” August 2025.

[7] Rolls-Royce SMR Limited, SMR0004520 Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 18: Human Factors,” August 2025.

[8] Rolls-Royce SMR Limited, SMR0004363, Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 23: Structural Integrity,” August 2025.

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

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

[11] Rolls-Royce SMR Limited, SMR0023654, “Risks, Assumptions, Issues, Dependencies & Oportunities Log (RAIDO),” This is a live tracking database.

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

[13] Rolls-Royce SMR Limited, SMR0024143, Issue 1, “Assumptions and Commitments Log,” not yet issued.

[14] Rolls-Royce SMR Limited, SMR0004293, Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 33: Safeguards,” August 2025.

[15] Office For Nuclear Regulation, Issue 9, “Nuclear Industries Security Regulations 2003 - Classification Policy for Civil Nuclear Industry,” Ocober 2024.

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

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

[18] Rolls-Royce SMR Limited, SMR0004542, Issue 4, “Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 2: Generic Site Characteristics,” August 2025.

[19] Rolls-Royce SMR Limited, SMR0009697, Issue 2, “Rolls-Royce SMR: Secure by Design Report,” February 2024.

[20] Rolls-Royce SMR Limited, SMR0009686, Issue 2, “Rolls-Royce SMR: Theft of Material and Categorisation Report,” January 2025.

[21] Rolls-Royce SMR Limited, SMR0009698, Issue 2, “Rolls-Royce SMR: Cyber Security Report,” February 2025.

[22] Rolls-Royce SMR Limited, SMR0009689, Issue 2, “Rolls-Royce SMR: Vital Area Identification and Categorisation Report,” February 2024.

[23] Rolls-Royce SMR Limited, SMR0009908, Issue 2, “Rolls-Royce SMR: Integrated Security Solution,” March 2025.

[24] International Atomic Energy Agency, INF CIRC/274, “Convention on the Physical Protection of Nuclear Material (as amended),” October 2021 .

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

[26] 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,” 2019.

[27] 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.

[28] International Atomic Energy Agency, IAEA Nuclear Security Series No. 48-T, “Identification and Categorisation of Sabotage Targets and Identification of Vital Areas at Nuclear Facilities,” 2024.

[29] Office for Nuclear Regulation, 2014 Edition, “Safety Assessment Principles for Nuclear Facilities, Revision 1,” January 2020.

[30] Office for Nuclear Regulation, Security Assessment Principles for the CIvil Nuclear Industry, Official Sensitive Annexes, Version 1.1, 2022 Edition.

[31] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-6.1, Issue 2.1, “Categorisation for Theft,” April 2025.

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

[33] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-7.1, Issue 2, “Effective Cyber and Information Management,” September 2024.

[34] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-11.4.1, Issue 1.1, “Secure by Design,” January 2023.

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

[36] 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.

[37] Rolls-Royce SMR Limited, SMR0001603, Issue 2, “Rolls-Royce SMR Environment, Safety, Security and Safeguards Design Principles,” July 2024.

[38] Rolls-Royce SMR Limited, SMR0005789, Issue 2, “Rolls-Royce SMR: Secure By Design Methodology,” August 2024.

[39] National Protective Security Authority, “NPSA Extranet - Threat Reports [online],” Available: https//extranet.npsa.go.uk/threats/threat-reports.

[40] 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].

[41] Rolls-Royce SMR Limited, SMR0006518, Issue 2, “Rolls-Royce SMR Environment, Safety, Security and Safeguards Categorisation and Classification Methodology,” July 2023.

[42] Rolls-Royce Limited, EDNS01000760628, Issue 2, “Secure by Design - Guidance Document: Principles and Method,” 2020.

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

[44] Rolls-Royce SMR Limited, SMR0006431, Issue 3, Rolls-Royce SMR: Cyber Security Risk Assessment Methodology, September 2024.

[45] National Insitute for Standards and Technology, Version 2.0, "The NIST Cybersecurity Framework (CSF) 2.0," Available: https://www.nist.gov/cyberframework, February 2024.

[46] Rolls-Royce SMR Limited, IMS Process C3.2.2-3, "Engineer Safe, Secure ,Safeguarded and Environmentally Sound Products," April 2025.

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

[48] Rolls-Royce SMR Limited, SMR0006499, Issue 2, "Rolls-Royce SMR: Vital Area Identification and Categorisation Methodology," August 2024.

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

[50] Rolls-Royce SMR Limited, IMS Process C3.2.1-9, "Manage Change," April 2025.

[51] Rolls-Royce SMR Limited, IMS Process C3.1.1, "Define and Manage Requirements," April 2025.

[52] Rolls-Royce SMR Limited, SMR0009132, Issue 1, "Environment, Safety, Security and Safeguards (E3S) Requirements and Analysis Arrangements," November 2023.

[53] Rolls-Royce SMR Limited, IMS Process C3.2.1-2, "Definition Review Process," April 2025.

[54] Rolls-Royce SMR Limited, SMR0022744, "Secure by Design Database," this is a live tracking document.

[55] Rolls-Royce SMR Limited, SMR0004210, Issue 4, Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 4: Reactor (Fuel and Core), August 2025.

[56] Rolls-Royce SMR Limited, SMR0004750, Issue 2, E3S Basic Technical Characteristics: Safeguards, January 2024.

[57] Rolls-Royce SMR Limited, SMR0004502, Issue 4, Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 11: Management of Radioactive Wastes, August 2025.

[58] Rolls-Royce SMR Limited, SMR0001122, Issue 2, Solid Operational Waste Identification, November 2023.

[59] International Atomic Energy Agency, RG-G-1.9, Categorisation of Radioactive Sources Safety Guide, 2005.

[60] Rolls-Royce SMR Limted, SMR0020549, Issue 1, "Cyber Security Design Requiremnts Specification," April 2025.

[61] 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.

[62] British Standards Institute, IEC62645, "Nuclear Power Plants- Instrumentation, Control and Electrical Power Systems - Cyber Security Requirements," 2020.

[63] Rolls-Royce SMR Limited, SMR0020085, Issue 1, "Rolls-Royce SMR: Reactor Protection System Cyber Security Risk Assesment Report," February 2025.

[64] Rolls-Royce SMR Limited, SMR0014713, Issue 1, Rolls-Royce SMR: Diverse Protection System Cyber Security Risk Assessment Report, February 2025.

[65] Rolls-Royce SMR Limited, SMR0020485, Issue 1, Rolls-Royce SMR Reactor Plant Control System Cyber Security Risk Assessment Report, February 2025.

[66] Rolls-Royce SMR Limited, SMR0020486, Issue 1, Rolls-Royce SMR: Data Processing & Control System Cyber Security Risk Assessment Report, February 2025.

[67] Rolls-Royce SMR Limited, SMR0003771, Issue 4, Environment, Safety, Security and Safeguards Case Version 3, Tier 1, Chapter 6: Engineered Safety Features, August 2025.

[68] Rolls-Royce SMR Limited, SMR0001389, Issue 4, Definition of Postulated Initiating Event Frequencies, February 2025.

[69] Rolls-Royce SMR Limited, SMR0004444, Issue 3, Rolls-Royce SMR Fault Schedule (Version 8), February 2025.

[70] Rolls-Royce SMR Limited, SMR0010027, Issue 2, Design Basis Radiological Consequence Analysis Modelling, October 2024.

[71] Rolls-Royce SMR Limited, SMR0007629, Issue 2, Severe Accident Off-site Consequences Methodology, September 2024.

[72] Rolls-Royce SMR Limited, SMR0021564, Issue 1, Rolls-Royce SMR: Blended Attack Framework, March 2025.

[73] Rolls-Royce SMR, SMR0020318, Issue 1, "Vital Area Identification and Categorisation Analysis - Reactivity Control," January 2025.

[74] Rolls-Royce SMR Limited, SMR0020316, Issue 1, "Vital Area Identification and Categorisation Analysis - Reactor Coolant," January 2025.

[75] Rolls-Royce SMR Limited, SMR0020314, Issue 1, "Vital Area Identification and Categorisation Analysis - Steam and Feed," January 2025.

[76] Rolls-Royce SMR Limited, SMR0023684, Issue 1, "Vital Area Identification and Categorisation Analysis - Containment Systems," in preparation.

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

[78] National Protective Security Authority, "Operational Requirements Guidance," 2018.

[79] National Cyber Security Centre, "Advice and Guidance," [Online]. Available: https://www.ncsc.gov.uk/section/advice-guidance/all-topics.

[80] L P C, "RedBook Live [online]," https://www.redbooklive.com/. [Online]. Available: https://www.redbooklive.com/.

[81] 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.

[82] Office For Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-9.2, Issue 2, "Local Police Forces," May 2024.

[83] Office for Nuclear Regulation, Technical Assessment Guide, CNS-TAST-GD-9.1, Issue 2, "CNC Response Force," May 2024.

[84] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-9.3, Issue 2, "Security Guard Services," May 2024.

[85] British Standards Insitute IEC 62443-3-3, "Industrial Communications Networks - Network & System Security - Part 3-3: System Security Requirements & Security Levels," 2013.

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

[87] Rolls-Royce SMR Limited, SMR0023683, Issue 1, "Physical Protection Systems - Operational Requirements," in preparation.

[88] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-6.6, "Adjacent or Enclave Nuclear Premises," 2022.

[89] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-10.1, Issue 3, "Counter Terrorism Measures EP&R Planning," September 2024.

[90] Office for Nuclear Regulation, Technical Assessment Guide CNS-TAST-GD-7.5, Issue 4, "Preparation for and Response to Cyber Security Incidents," January 2024.

32.13 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:

[Claim 32.1] 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 32.13-1.

Table 32.13-1: Nuclear Security Sub-claims - Secure by Design

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
[32.1.1] A set of credible Secure by Design principles have been published and have been applied to the design of the Rolls-Royce SMR.	[32.1.1.1] The Secure by Design principles are credible.	*Not used at Version 3 of the E3S Case*
	[32.1.1.2] The Secure by Design principles have been published and communicated to designers.	*Not used at Version 3 of the E3S Case*
	[32.1.1.3] The Secure by Design principles have been applied to the Rolls-Royce SMR design.	*Not used at Version 3 of the E3S Case*
	[32.1.1.4] Security vulnerabilities have been reduced as a result of applying the Secure by Design principles.	*Not used at Version 3 of the E3S Case*
[32.1.2] A credible Secure by Design methodology has been applied to the design of the Rolls-Royce SMR.	[32.1.2.1] The Secure by Design Methodology is credible.	[32.1.1.4] Where improvements to the methodology are identified during its application or analysis these are fed back to the methodology author.
	[32.1.2.2] The Secure by Design Methodology has been applied to the RR SMR.	[32.1.2.2.1] An initial security assessment of the design has been undertaken to identify sources of security risk.
		[32.1.2.2.2] Design changes that eliminate or reduce sources of security risk inherent in the design have been recommended.

Nuclear Security Subclaims Level 2	Nuclear Security Sub-claims Level 3	Nuclear Security Sub-claims Level 4
	[32.1.2.3] Security vulnerabilities have been reduced by applying the Secure by Design Methodology.	[32.1.2.3.1] Recommended design changes have been screened for their impact to safety and operation of the RR SMR.
		[32.1.2.3.2] Screened and accepted design changes have been incorporated into the design.
[32.1.3] Security considerations have been integrated into the design process.	[32.1.3.1] There are requirements for security.	*Not used at Version 3 of the E3S Case*
	[32.1.3.2] Security is considered in design optioneering.	*Not used at Version 3 of the E3S Case*
[32.1.1] A set of credible Secure by Design principles have been published and have been applied to the design of the Rolls-Royce SMR.	[32.1.1.1] The Secure by Design principles are credible.	*Not used at Version 3 of the E3S Case*
	[32.1.1.2] The Secure by Design principles have been published and communicated to designers.	*Not used at Version 3 of the E3S Case*
	[32.1.1.3] The Secure by Design principles have been applied to the Rolls-Royce SMR design.	*Not used at Version 3 of the E3S Case*
	[32.1.1.4] Security vulnerabilities have been reduced as a result of applying the Secure by Design principles.	*Not used at Version 3 of the E3S Case*
[32.1.2] A credible Secure by Design methodology has been applied to the design of the Rolls-Royce SMR.	[32.1.2.1] The Secure by Design Methodology is credible.	[32.1.1.4] Where improvements to the methodology are identified during its application or analysis these are fed back to the methodology author.
	[32.1.2.2] The Secure by Design Methodology has been applied to the RR SMR.	[32.1.2.2.1] An initial security assessment of the design has been undertaken to identify sources of security risk.
		[32.1.2.2.2] Design changes that eliminate or reduce sources of security risk inherent in the design have been recommended.

Nuclear Security Subclaims Level 2	Nuclear Security Sub-claims Level 3	Nuclear Security Sub-claims Level 4
	[32.1.2.3] Security vulnerabilities have been reduced by applying the Secure by Design Methodology.	[32.1.2.3.1] Recommended design changes have been screened for their impact to safety and operation of the RR SMR.
		[32.1.2.3.2] Screened and accepted design changes have been incorporated into the design.

32.14 Appendix B: Nuclear Security Sub-claims - Categorisation for Theft

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

[32.2] Material at risk of theft is identified. Security measures are identified, and applied in a Graded Approach, to minimise the risk of theft.

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 - Categorisation for Theft

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
[32.2.1] The Nuclear Material (NM) & Other Radioactive Material (ORM) inventories are categorised, methodology, for the purpose of identifying the level of protection from theft that is required.	[32.2.1.1] – The inventory of Nuclear Material (NM) and Other Radioactive Material (ORM) is established for the generic RR SMR.	*Not used at Version 3 of the E3S Case*
	[32.2.1.2] - Targets (and their locations) which require protection against theft are identified and categorised against relevant regulatory criteria	*Not used at Version 3 of the E3S Case*
[32.2.2] The relevant security outcomes and requirement for protection for the categorised NM & ORM are established.	[32.2.2.1] Any applicable recommendations to reduce risk of theft of NM & OPM are proposed a part of the Secure by Design Approach	*Not used at Version 3 of the E3S Case*
	[32.2.2.2] Security measures to protect against theft of NM & ORM are identified, and applied in a Graded Approach, to minimise the risk of theft.	[32.2.2.2.1] Security measures to protect against theft of NM are identified and are incorporated into the Integrated Security Solution (ISS) for the generic RR SMR.
		[32.2.2.2.2] Security measures to protect against theft of discrete nuclear sources are identified and are incorporated into the Integrated Security Solution (ISS) for the generic RR SMR

Nuclear Security Subclaims Level 2	Nuclear Security Sub-claims Level 3	Nuclear Security Sub-claims Level 4
		[32.2.2.2.3] Security functions to protect against theft of ORM; with security measures providing such are incorporated into the Integrated Security Solution (ISS) for the generic RR SMR.

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

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

[32.3] Effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology (including Information Technology (IT) and Operational Technology (OT)) have been implemented and maintained.

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 - Cyber Security and Information Assurance

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
[32.3.1] A Cyber Protection System, including policies and procedures, is in place to manage cyber risk in accordance with recognised international standards and RGP	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*
[32.3.2] Computer-Based Systems are risk assessed using a consequence-based risk assessment process and assigned a security degree	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*
[32.3.3] Mitigations to cyber security risks are proportionally applied using a graded approach	[32.3.3.1] Cyber security risks to Computer-based Systems that could result in an Unacceptable Radiological Consequence shall be mitigated to an acceptable level.	*Not used at Version 3 of the E3S Case*
	[32.3.3.2] Cyber security risks to Computer-based Systems that could result in the theft of nuclear material and other radiological material shall be mitigated to an acceptable level.	*Not used at Version 3 of the E3S Case*
	[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	*Not used at Version 3 of the E3S Case*

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
[32.3.4] The effectiveness of the cyber protection system is verified and validated	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*
[32.3.5] Sensitive Information is subject to appropriate security controls to maintain its confidentiality, integrity and availability	[32.3.5.1] Cyber security risks associated with the compromise of SNI are mitigated to an acceptable level.	*Not used at Version 3 of the E3S Case*
	[32.3.5.2] Assets storing or transmitting Sensitive Information are protected physically by the PPS	*Not used at Version 3 of the E3S Case*
[32.3.6] The Cyber Protection System, as part of the ISS, includes measures to ensure that systems are designed to be secure and resilient against the cyber threat, as defined by the DBT, throughout their lifecycle stages	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*
[32.3.7] The CPS provides the software, tools and architecture to enable detection, response and recovery from cyber incidents	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*

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

Vital Area Identification &Classification is the subject of a Level 1 security specific E3S sub-claim, as follows:

[Claim 32.4] The threat of sabotage of the Rolls-Royce SMR is minimised through the development of proportionate security measures as part of a Physical Protection System (PPS) which is included within an Integrated Security Solution (ISS).

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.

Table 32.16-1: Nuclear Security Sub-claims - Vital Area Identification and Categorisation

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
[32.4.1] The design basis threat of the sabotage of nuclear material or other radioactive material which could result in Unacceptable Radiological Consequence is 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.	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*
[32.4.2] 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.	[32.4.2.1] The Vital Area Identification and Categorisation methodology identifies potential threats from physical, cyber or blended attack which could result in an Unacceptable Radiological Consequence (URC).	*Not used at Version 3 of the E3S Case*
	[32.4.1.2] – 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.	*Not used at Version 3 of the E3S Case*

Nuclear Security Subclaims Level 2	Nuclear Security Sub-claims Level 3	Nuclear Security Sub-claims Level 4
	[32.4.2.3] – 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 where their compromise could be part of a blended attack	*Not used at Version 3 of the E3S Case*
	[32.4.2.4] 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.	*Not used at Version 3 of the E3S Case*
	[32.4.2.5] 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).	*Not used at Version 3 of the E3S Case*
	[32.4.2.6] 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.	*Not used at Version 3 of the E3S Case*

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
	[32.4.2.7] Vital Areas have been established based on the Targets (NM/ORM and preventative / protective /mitigating SSCs) requiring protection from sabotage and their locations.	*Not used at Version 3 of the E3S Case*
[32.4.3] 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.	[32.4.3.1] 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) and sought to influence design in order to reduce the risk. This includes influence on site layout modularisation and the (Safety Case) requirements for segregation and diversity.	*Not used at Version 3 of the E3S Case*
	[32.4.3.2] 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.	*Not used at Version 3 of the E3S Case*
	[32.4.3.3] 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.	*Not used at Version 3 of the E3S Case*
	[32.4.3.4] The application of Secure by Design has resulted in the reduction of the vulnerability of SSCs from sabotage, and the minimisation of the number of Vital Areas, and (where practical) a reduction in the categorisation.	*Not used at Version 3 of the E3S Case*

Nuclear Security Subclaims Level 2	**Nuclear Security Sub-claims Level 3**	**Nuclear Security Sub-claims Level 4**
	[32.4.3.5] The application of Secure by Design further supports the prevention of non-nuclear related threats from sabotage to SSCs as a result of a physical, cyber or blended attack.	*Not used at Version 3 of the E3S Case*
[32.4.3] The security solutions to address the sabotage risk (from physical, cyber or blended attack) to RR SMR are developed and included with the Integrated Security Solution.	*Not used at Version 3 of the E3S Case*	*Not used at Version 3 of the E3S Case*

32.17 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:

[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 32.17-1

Table 32.17-1: Nuclear Security Sub-claims - Integrated Security Solution

Nuclear Security Sub-Claims Level 2	**Nuclear Security Sub-Claims Level 3**	**Nuclear 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),	[32.5.1.2.1] Defines the level of physical protection provided

Nuclear Security Sub-Claims Level 2	Nuclear Security Sub-Claims Level 3	Nuclear Security Sub-Claims Level 4
	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).	within the design, based on the output of Security Analyses (e.g. VAI&C, Theft and Vulnerability Assessment) against the Final Concept Design (FCD).
		[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

Nuclear Security Sub-Claims Level 2	Nuclear Security Sub-Claims Level 3	Nuclear Security Sub-Claims Level 4
		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.
		[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.
		[32.5.1.3.5] Demonstrates the concept selection and optioneering of the cyber protection solutions meet the desired outcome through,

Nuclear Security Sub-Claims Level 2	Nuclear Security Sub-Claims Level 3	Nuclear Security Sub-Claims Level 4
		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 used at Version 3 of the E3S Case*
	[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 used at Version 3 of the E3S Case*
	[32.5.2.3] The ISS considers all Operational states, including normal power production and routine outages.	*Not used at Version 3 of the E3S Case*
	[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 used at Version 3 of the E3S Case*

Nuclear Security Sub-Claims Level 2	Nuclear Security Sub-Claims Level 3	Nuclear Security Sub-Claims Level 4
	[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.

32.18 Appendix F: Integration between Security and Other Topic Areas

Table 32.18-1: Integration between Security and Other Topic Areas

E3S Chapter	Outline Scope of Topic Area	Interaction with Ch 32
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) are being 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 are being 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 –also informs 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.	
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

E3S Chapter	Outline Scope of Topic Area	Interaction with Ch 32
		Good Practice (RGP) and Operating Experience (OPEX). The application of the Cyber Security Risk Assessment Methodology to these C&I systems 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 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.
Chapter 9A:	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	The civil and structural designs will be reviewed against the adversary capabilities described in the Threat Interpretation document. Potential security vulnerabilities will be identified

E3S Chapter	Outline Scope of Topic Area	Interaction with Ch 32
	protection against external hazards.	and presented to the structural engineers to design out, and the Security Case 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.	Radioactive waste is a potential target for heft and sabotage.
Chapter 12: Radiation Protection	Evaluates how radiation doses to onsite workers and members of the public will be controlled during normal operations and describes the design features of the RR SMR that minimise exposures to ALARP.	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 Security Case 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 Security Case will link into Section 13.2 – Nuclear Safety and Security Interfaces – of the Chapter.

E3S Chapter	Outline Scope of Topic Area	Interaction with Ch 32
Chapter 15: Safety Analysis	Presents the methods and outputs of the safety analysis that evaluate the RR SMR against relevant criteria and inform the design development, including the deterministic analysis of faults and accidents, probabilistic analysis, and internal and external hazard assessment.	The outputs from the Safety Analysis will be key inputs to develop Candidate IEMOs and Candidate Sabotage 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 (OLC) 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 OLC, will be used in the Security Case 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 19: Emergency Preparedness and Response	Discusses the design and arrangements for preparedness and response to nuclear or radiological emergencies.	The design of integrated PPS and CPS within the ISS should support (and minimise conflict) with emergency arrangements and planning. For example, the access control system could aid in the location and search for unaccounted personnel in the event of an emergency.
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 Ch 32
		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 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.

32.19 Abbreviations

ALARP	As Low As Reasonably Practicable
BAT	Best Available Techniques
BEIS	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
CDT	Central Dependency Table
CfT	Categorisation for Theft
C&I	Control and Instrumentation
CNI	Critical National Infrastructure
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRE	Control of Radiation Exposure
CoRM	Confinement of Radioactive Material
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
DiD	Defence in Depth
DPCS	Data Processing and Control System
DPS	Diverse Protection System
DR	Definition Review
DRP	Design Reference Point
E3S	Environment, Safety, Security and Safeguards

ECC	Emergency Control Centre
EMIT	Examination, Maintenance, Inspection, and Testing
EP&R	Emergency Preparedness and Response
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
GDF	Geological Disposal Facility
HCE	High Consequence Event
HCVA	High Consequence Vital Area
HF	Human Factors
HVM	Hostile Vehicle Mitigation
HVAC	Heating, Ventilation and Air Conditioning
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) Key Security Plan Principle
LLW	Low Level Waste
MCR	Main Control Room

NISR 2003	Nuclear Industries Security Regulations 2003
NIST	National Institute for Standards and Technology
NSL	Nuclear Site Licence
NM	Nuclear Material
NPSA	National Protective Security Authority
NSSP	Nuclear Site Security Plan
NSV	National Security Vetting
OLC	Operating Limits and Conditions
ONR	Office for Nuclear Regulation
ONRCNSS	Office for Nuclear Regulation Civil Nuclear Security and Safeguards
OP&R	Outcome, Posture and Response
OR	Operational Requirements
ORM	Other Radioactive Material
OT	Operational Technology
PAA	Preliminary Assumption-based Assessment
PCD	Preliminary Concept Definition
PSES	Potential Sabotage Event Scenario
PPS	Physical Protection System
PWR	Pressurised Water Reactor
RAIDO	Risks, Assumptions, Issues, Dependencies and Opportunities
RASyP	(ONR) Regulatory Assessment of Security Plans
RD	Reference Design
RDS-PP®	Reference Designation System for Power Plants
RGP	Relevant Good Practice
RPCMS	Reactor Plant Control & Monitoring System
RPCPS	Reactor Control and Protection System
RPCS	Reactor Plant Control System
RPS	Reactor Protection System

RR SMR	Rolls-Royce Small Modular Reactor
RWMA	Radioactive Waste Management Arrangements
SAPs	(ONR) Safety Assessment Principles
SbyD	Secure by Design
SCP	Security Contingency Plan
SCR	Supplementary Control Room
SD	Security Degree
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
SSCs	Structures, Systems, Components
SOPR	Security Outcomes Postures and Responses
SPND	Self-powered Neutron Detectors
SSyP	SMR Security Principle
SuC	System under Consideration
SyAPs	Security Assessment Principles
SyCC	Security Control Centre
SyDP	(ONR) Security Delivery Principles
TAG	(ONR) Technical Assessment Guide
UK	United Kingdom
URC	Unacceptable Radiological Consequence
VA	Vital Area
VAI&C	Vital Area Identification and Categorisation