HOLTEC BRITAIN

A Holtec International Company

Holtec Britain Ltd	HI-2240878
Sponsoring Company	**Document Reference**
0	23 September 2025
Revision No.	**Issue Date**
Report	Non-proprietary
Record Type	**Proprietary Classification**
ISO 9001	No
Quality Class	**Export Control Applicability**

Record Title:

Generic Security Report

Proprietary Classification

This record does not contain commercial or business sensitive information.

Export Control Status

Export Control restrictions do not apply to this record.

Revision Log

Revision	Description of Changes
0	First Issue to Regulators

Table of Contents

1.0 Introduction 5
1.1 Overview 5
1.2 Aim and Objectives of the GDA Step 2 Generic Security Report 5
1.3 Scope and Exclusions 6
1.4 GDA Step 2 Security Submissions 7
1.5 Structure of the Generic Security Report 9
2.0 Abbreviations 10
3.0 Legislative and Regulatory Framework 14
3.1 Introduction 14
3.2 International Regulation and Guidance 14
3.3 UK Regulation 15
3.4 ONR Guidance 15
4.0 Security Philosophy and Principles 19
4.1 Introduction 19
4.2 Security Philosophy 19
5.0 Scope of GDA and Plant Information 26
5.1 Scope 26
5.2 Plant Information 26
6.0 Nuclear Security Case 31
6.1 Introduction 31
6.2 Security Claims 32
6.3 Security Sub-Claims 32
6.4 Integration with the Safety, Environmental and Safeguards Case 33
6.5 Security Design Principles 33
7.0 Delivery of Security 34
7.1 Introduction 34
7.2 Identification of Nuclear Material, Other Radioactive Material and Sensitive Nuclear Information 34
7.3 Identification of Assets and Areas for Protection 35
7.4 Threat Information 38
7.5 Protection of Assets and Vital Areas 40
7.6 Security Operations 48
7.7 Application of the Secure by Design Principle 48
7.8 GDA Undertakings 49

7.9 Expectations on a Future Licensee 49
8.0 References 51
9.0 List of Appendices 55
Appendix A Compliance with the Nuclear Industries Security Regulations A-1
Appendix B Security Claims, Arguments and Evidence B-1
Appendix C Generic SMR-300 Candidate Vital Area Locations C-1
Appendix D Generic SMR-300 Illustrative Security Zones D-1
Appendix E Compliance with Fundamental Security and Security Delivery Principles E-1
Appendix F Demonstration of the Security 'Golden Thread' F-1

List of Figures

Figure 1: Step 2 GDA Security Documentation 7
Figure 2: Security Risk Control Enablers 20
Figure 3: Secure by Design Hierarchy of Risk Controls 21
Figure 4: Elements of a Security by Design Approach 22
Figure 5: Defence in Depth 24
Figure 6: Integrated Security Solution 25
Figure 7: Conceptual SMR-300 Layout 27
Figure 8: Delivery of Nuclear Security for the SMR-300 32
Figure 9: SMR-300 Security Case Aim and High-Level SyCs 32
Figure 10: Integration of the Security Case with the SSEC 33
Figure 11: SMR-300 Vital Area Identification and Categorisation Methodology 36
Figure 12: Sabotage Logic Model 37
Figure 13: Evolutionary Use of Threat in SMR-300 Security Assessments 38
Figure 14: GDA Step 2 Threat Development Methodology 39
Figure 15: Overview of Cyber Security Risk Assessment Methodology for Single Systems 41
Figure 16: Multi-System Justification Methodology 42
Figure 17: Development of Conceptual Security Arrangements during GDA 45

Figure 18: Development of Security Architecture in GDA 45

Figure 19: Generic SMR-300 Designated Areas (Example) 46

Figure 20: Outline Security Infrastructure Definition Approach 47

Figure 21: List N Pathway A-2

Figure 22: Key Elements of a Security Management System A-3

Figure 23: Security Claims and Sub-Claims B-2

Figure 24: Golden Thread F-2

List of Tables

Table 1: GDA Step 2 Security Submissions 8

Table 2: Structure of the GSR 9

Table 3: Preliminary Security Zones 47

Table 4: GDA Security Undertakings 49

Table 5: Expectations on a Future UK SMR-300 Licensee 49

Table 6: Pathway Activities A-3

Table 7: Security Arrangements and Compliance against SyAPs A-4

Table 8: Security Claims Map to GSR Section B-3

Table 9: Security Sub-Claim map to GSR Supporting Document B-3

1.0 INTRODUCTION

1.1 Overview

Holtec International (Holtec) is planning to deploy its 300 MWe Small Modular Reactor (SMR-300) in the United Kingdom (UK). To support this, Holtec (via its UK Division, Holtec Britain) has submitted its Generic SMR-300 design for Steps 1 and 2 of the Generic Design Assessment (GDA) process by the UK nuclear regulators, namely the Office for Nuclear Regulation (ONR), the Environment Agency (EA) and Natural Resources Wales (NRW).

The focus of the overall assessment in the two-step GDA is towards the fundamental adequacy of the design and the safety, security, safeguards, and environmental cases. From a security perspective, this includes determination of the suitability of the methodologies, approaches, codes, standards, and philosophies which form the building blocks for the assessments and the development of the Generic Security Report (GSR) in Step 2 (this document) and the subsequent site-specific security design.

During Step 1 of the GDA, the Preliminary Security Report (PSyR) [1] was developed to provide ONR with the confidence that it would be able to undertake a 'meaningful assessment' of the security topic during Step 2.

This GSR forms part of a suite of documents which together form the Safety, Security and Environmental Case (SSEC)[1] which have been developed during the course of the GDA and which, in general terms, set down the claims and arguments supporting the generic SMR-300 design for UK deployment. The contents of the SSEC address the following key aspects:

- Nuclear safety via the Preliminary Safety Report (PSR).
- Environmental protection via the Preliminary Environmental Report (PER).
- Safeguards (via the Preliminary Safeguards Report (PSgR).
- Security (via this GSR).

To ensure that the SSEC is balanced and integrates these four key aspects, the following fundamental purpose is defined in the PSR (Part A Chapter 3):

> *The Generic Holtec SMR-300 can be constructed, commissioned, operated and decommissioned on a generic site in the UK to fulfil the future licensee's legal duties to be safe, secure and protect people and the environment.*

1.2 Aim and Objectives of the GDA Step 2 Generic Security Report

This GSR represents an evolution of the GDA Step 1 PSyR and presents the (developing) Security Case for the Generic SMR-300.

The overall aim of this GSR and its supporting documents is to enable ONR to undertake a 'meaningful assessment' of the security topic to support the assessment of the fundamental

[1] The SSEC also includes the Preliminary Safeguards Report.

adequacy of the design and security case in GDA Step 2 and thereby contribute positively towards the ONR Step 2 public statement.

This aim is achieved through achieving the following GSR objectives:

1. Provide suitable and sufficient plant design and operation information (within the agreed GDA scope of assessment) to enable understanding of the GSR by a technical reader.
2. Demonstrate how the evolving design is compliant with the UK nuclear security regulatory framework.
3. Outline the security claims, arguments and evidence showing how these claims integrate with the overall high-level SMR-300 safety, security, safeguards and environmental claims.
4. Demonstrate how the security philosophy and principles are being adopted.
5. Present the key assessment methodologies (including methodologies for Vital Area Identification and Categorisation (VAI&C), Cyber Security Risk Assessment (CSRA), Threat Development and the application of Secure by Design (SbD)) and how they are being implemented.
6. Demonstrate how the nuclear security case and security arrangements are being developed.
7. Outline the evolution to site licensing and the Nuclear Site Security Plan (NSSP).

1.3 Scope and Exclusions

As originally defined by [1], the scope of the SMR-300 GDA Step 2 GSR is focused on the methodologies, approaches, codes, standards, and philosophies which together will form the building blocks for the development of the GSR and site security arrangements/security plan. The design under assessment is defined by the Design Reference Point (DRP) [2].

The GDA Step 2 scope includes an illustrative implementation of these methodologies to build confidence that they are suitable and sufficient for use in subsequent project stages. This assists ONR in their assessment that the methodologies proposed are adequate and, if implemented by a site licensee, would lead to an SMR-300 design compliant with legislative and regulatory requirements in the UK (as outlined in Section 3.0). The initial implementation of these methodologies in GDA Step 2 further assists ONR in confirming that they have not identified a fundamental shortfall from a security perspective within the constraints of GDA Step 2.

The following are excluded from the GSR scope and will be addressed during the site-specific assessment phase:

- Facilities, buildings, operations or systems not identified in the GDA Scope [3].
- Sensitive Nuclear Information (SNI) located on a future SMR-300 site.
- Assessment of malicious aircraft impact, which is addressed by PSR Chapter B21.
- The provision of equipment for safeguards purposes (this is addressed by the PSgR [4]).

The depth of security assessment is commensurate with the maturity of the plant design at GDA Step 2.

1.4 GDA Step 2 Security Submissions

An outline of the Step 2 GDA security submissions was first introduced in the Step 1 PSyR [1].

In total, ten documents support the nuclear security element of the GDA in Step 2[2]. These comprise the GSR itself (this document) together with nine supporting reports as illustrated in Figure 1 below. The structure of this pyramid reflects the claims, argument and evidence structure of the GSR suite of documents.

At the top is this claims-level GSR, with the middle layer being argument level documents, such as methodologies. The lower tier represents the evidence documents which detail the assessments undertaken. In GDA Step 2, several documents combine methodology and assessment because of their relatively high level nature and are shown in Figure 1 as combining argument and evidence.

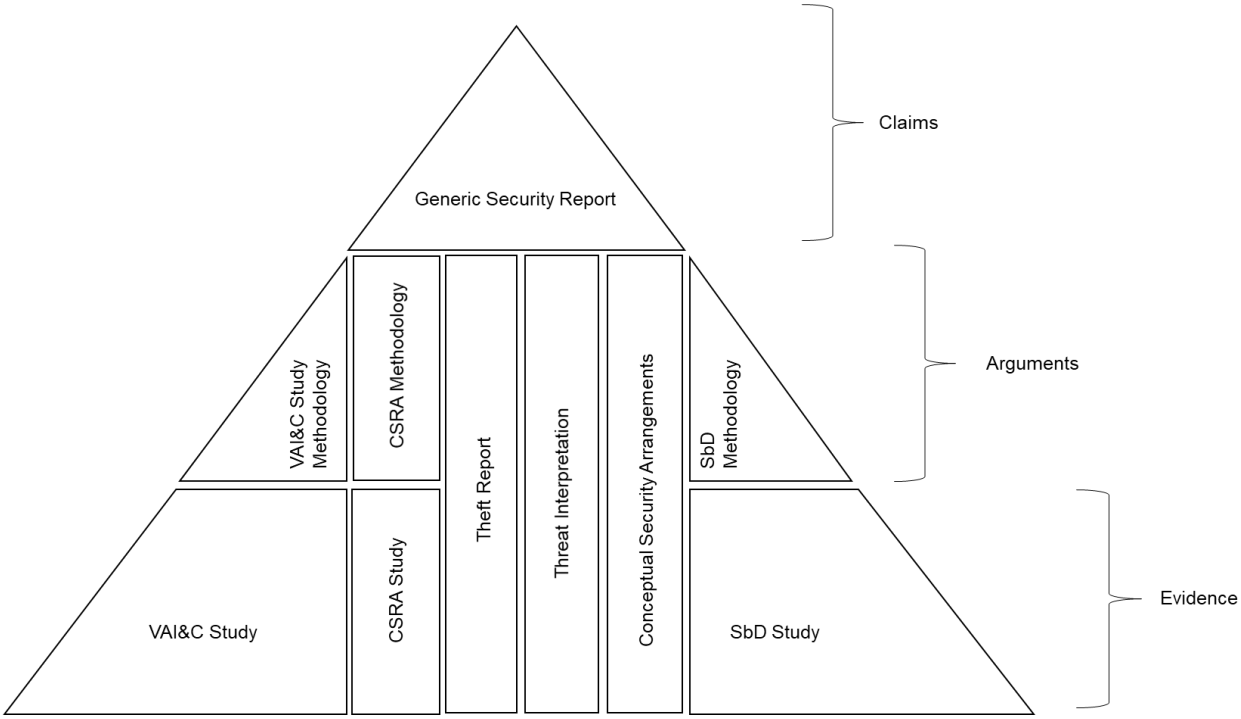

Figure 1: Step 2 GDA Security Documentation

A summary of the contents of each of these security submissions is provided below in Table 1. The Security Classification of each document has been reviewed relative to the Holtec Britain Classification Policy and Guidance Document [5] prior to issue and is shown in Table 1 below.

[2] There will also be a redacted version of the GSR produced for the public consultation website.

Table 1: GDA Step 2 Security Submissions

Step 2 Submission	Synopsis	Document Security Classification
GSR	This is the head security document. It presents the overall nuclear security case and how the evolving design is compliant with the UK nuclear security framework and meeting the security objectives.	OFFICIAL-SENSITIVE (O-S):SNI
GSR (Public)	This is a public version of the GSR suitable for the SMR-300 GDA public consultation website.	OFFICIAL
VAI&C Methodology Report	This document describes the methodology to be used to identify and categorise the Generic SMR-300 Vital Areas.	OFFICIAL
CSRA Methodology Report	This document describes the methodology to be used for the CSRA of the Generic SMR-300 digital systems.	OFFICIAL
SbD Methodology Report	This document identifies the role of SbD within the project and develops an SbD framework for GDA Step 2 and beyond.	OFFICIAL
GDA Step 2 Threat Report	This document describes the GDA Step 2 threat development methodology and presents the threat information for use in the GDA VAI&C and CSRA GDA studies based on a generic threat.	O-S:SNI
Theft Methodology and Analysis Report	This document presents the methodology for determining the classification for theft for the Generic SMR-300 plant. It also reports an initial theft assessment for Step 2.	O-S:SNI
VAI&C Study Report	This document presents a VAI&C study focused on the Nuclear Material/Other Radioactive Material (NM/ORM) within the Containment Structure to: (1) demonstrate the implementation of the VAI&C methodology (2) inform the security design of the SMR-300 and (3) inform the derivation of conceptual physical security posture and response outcomes. The report also presents a high level judgement based qualitative VAI review for the NM/ORM in other areas within the plant to enable ONR to do a meaningful Step 2 assessment and which supports (2) and (3) above.	O-S:SNI
CSRA Study Report	This document presents a CSRA study on the Generic SMR-300 Plant Safety System (PSS) to: (1) demonstrate the implementation of the CSRA methodology (2) inform the security design of the SMR-300 and (3) inform the derivation of conceptual cyber-security posture and response outcomes for the selected system.	O-S:SNI
SbD Report	This document presents the implementation of SbD during GDA through application of the SbD Methodology. It provides examples and evidence of application of SbD within the evolving design of the SMR-300 up to the end of GDA Step 2.	O-S:SNI
Conceptual Security Arrangements Report	This document presents a high-level overview of the expected security architecture, security infrastructure and concept of security operations commensurate with the level of design development and security assessment undertaken at GDA Step 2. This is intended to provide the future site licence holder with the basis for the development of the site-specific security plans.	O-S:SNI

1.5 Structure of the Generic Security Report

This GSR delivers its objectives as identified in Table 2:

Table 2: Structure of the GSR

Section	Presents:	GSR Objective(s)
3.0	Holtec Britain's understanding of the international and UK legislative and regulatory framework for nuclear security	2
4.0	The philosophy and principles which will be applied to develop the Generic SMR-300 nuclear security case	4
5.0	Scope of the GDA and plant information for the Generic SMR-300	1
6.0	Outline of the Generic SMR-300 security case	3
7.0	Delivery of security	4, 5, 6, 7

2.0 ABBREVIATIONS

Term	Definition
ACP	Access Control Point
ADS	Automatic Depressurisation System
ALARP	As Low as Reasonably Practicable
AR	Annular Reservoir
BAP	Breathing Air and Pressurisation System
BTP	British Transport Police
CAE	Claims, Argument, Evidence
CBSIS	Computer Based Systems Important to Safety
CBSy	Computer Based Security Systems
CBV	Containment Ventilation System
CES	Containment Enclosure Structure
CGC	Combustible Gas Control System
CNC	Civil Nuclear Constabulary
CNSC	Canadian Nuclear Safety Commission
CNSS	Civil Nuclear Security and Safeguards
CONOP	Concept of Security Operations
CPM	Cyber Protective Measure
CPPNM	Convention on the Physical Protection of Nuclear Material
CPS	Cyber Protection System
CREZ	Control Room Emergency Zone
CS&IA	Cyber Security & Information Assurance
CS	Containment Structure
CSA	Conceptual Security Arrangements
CSH	Overhead Heavy Load Handling System
CSRA	Cyber Security Risk Assessment
CVC	Chemical and Volume Control System
CWS	Chilled Water System
DBA	Design Basis Accident
DBT	Design Basis Threat
DESNZ	Department for Energy Security & Net Zero
DRP	Design Reference Point
EA	Environment Agency
EE	Evidencing Expectation
EP&R	Emergency Preparedness and Response
ESF	Engineered Safety Feature
FHA	Fuel Handling Area
FMEA	Failure Modes and Effects Analysis
FSyP	Fundamental Security Principle
GB GSE	Great Britain Generic Site Envelope

Term	Definition
GDA	Generic Design Assessment
GSR	Generic Security Report
HCVA	High Consequence Vital Area
HMG	His Majesty's Government
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IB	Intermediate Building
ICSANT	International Convention for the Suppression of Acts of Nuclear Terrorism
IEMO	Initiating Event of Malicious Origin
IRP	Inherent Risk Profile
ISFSI	Independent Spent Fuel Storage Installation
ISS	Integrated Security Solution
JBVAI	Judgement-Based Vital Area identification
KSyPP	Key Security Plan Principle
LLH	Light Load Handling System
LOCA	Loss of Coolant Accident
MCH	MCR Habitability System
MCR	Main Control Room
MPC	Multi-Purpose Canister
MWe	Mega Watt Electric
NCSC	National Cyber Security Centre
NFSV	New Fuel Storage Vault
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NMAC	Nuclear Material Accounting and Control
NPSA	National Protective Security Authority
NRC	Nuclear Regulatory Commission
NRW	Natural Resources Wales
NSS	Nuclear Security Series
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
O-S	Official-Sensitive
PCC	Passive Core Cooling System
PCM	Passive Core Makeup Water System
PDH	Primary Decay Heat Removal System
PER	Preliminary Environmental Report
PPM	Physical Protective Measure
PPS	Physical Protection System

Term	Definition
PSA	Probabilistic Safety Assessment
PSES	Potential Sabotage Event Scenario
PSgR	Preliminary Safeguards Report
PSyR	Preliminary Security Report
PSR	Preliminary Safety Report
PSS	Plant Safety System
PWR	Pressurised Water Reactor
RAB	Reactor Auxiliary Building
RCA	Radiologically Controlled Area
RCCA	Rod Cluster Control Assembly
RGP	Relevant Good Practice
RHR	Residual Heat Removal System
RP	Requesting Party
RPV	Reactor Pressure Vessel
RR SMR	Rolls-Royce Small Modular Reactor
RSF	Remote Shutdown Facility
S	Secret
SA	Security Architecture
SbD	Secure by Design
SD	Security Degree
SDH	Secondary Decay Heat Removal System
SDS	Sabotage Damage State
SES	Sabotage Event Scenario
SFP	Spent Fuel Pool
SI	Security Infrastructure
SIRO	Senior Information Risk Owner
SLM	Sabotage Logic Model
SME	Subject Matter Expert
SMR	Small Modular Reactor
SMR-300	300 MWe Small Modular Reactor
SNI	Sensitive Nuclear Information
SORP	Security Outcomes, Responses and Postures
SPF	Security Policy Framework
SSC	Structure, System and Component
SSEC	Safety, Security and Environmental Case
SyAP	Security Assessment Principle
SyC	Security Claim
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide
TB	Turbine Building
TIG	Technical Inspection Guide

Term	Definition
URC	Unacceptable Radiological Consequence
UK	United Kingdom of Great Britain and Northern Ireland
UMAX	Underground Maximum Capacity
US	United States of America
VAI&C	Vital Area Identification and Categorisation
VBIED	Vehicle-Borne Improvised Explosive Device
VDR	Vendor Design Review
VVM	Vertical Ventilated Module
WENRA	Western European Nuclear Regulators Association

3.0 LEGISLATIVE AND REGULATORY FRAMEWORK

3.1 Introduction

This section summarises international and UK regulation and guidance which inform Holtec Britain's understanding of the requirements and expectations for nuclear security for the SMR-300 in the UK and hence are reflected by the philosophies, principles and approaches outlined in this GSR.

3.2 International Regulation and Guidance

The UK is signatory to two international conventions which are relevant to the legislative framework for the protection of Nuclear Material (NM), Other Radioactive Material (ORM) and SNI:

a) As a member state of the International Atomic Energy Agency (IAEA) and a signatory to the Convention on the Physical Protection of Nuclear Material (CPPNM) [6] and its amendment [7]), the UK is obliged to establish and maintain a framework which provides for the application of physical protection requirements and include a system of evaluation, permissioning and compliance inspection, together with a means of enforcement, including effective sanctions.
b) The United Nations International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) [8]. In particular, Article 8 requires signatories to make every effort to adopt appropriate measures to ensure the protection of radioactive material, considering recommendations and functions of IAEA.

Furthermore, both conventions refer to the IAEA and the relevant guidance which it provides in these areas.

IAEA's objective for a State's nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event. To achieve this objective, a State should establish, implement, maintain, and sustain an effective and appropriate nuclear security regime to prevent, detect and respond to such nuclear security events.

Within IAEA, the Nuclear Security Series (NSS) provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The series comprises four sets of publications:

- Nuclear Security Fundamentals [9], which establishes the fundamental objective and essential elements of a State's national nuclear security regime.
- Recommendations, which set out measures that States should take 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.

Of relevance to a security submission during GDA are:

- Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities, NSS No 13 (INFCIRC225 Revision 5) [10].
- Identification and Categorization of Sabotage Targets and identification of Vital Areas at Nuclear Facilities, NSS No 48-T [11].
- Computer Security of Instrumentation and Control Systems at Nuclear Facilities, NSS No 33-T [12].

In addition, the Western European Nuclear Regulators Association (WENRA) has published guidance on the interfaces between nuclear safety and nuclear security [13] which provides recommendations for promoting synergy between safety and security assessments, resolving conflicts and the importance of the application of a security by design philosophy early in the design of new plants.

3.3 UK Regulation

In the UK, these international obligations are currently achieved primarily through two pieces of legislation, namely:

- The Energy Act (2004) defines the provisions which establish ONR as a statutory body, describes its purposes (one of which is nuclear security) and establishes its powers.
- The Nuclear Industries Security Regulations (NISR) 2003.

The regulations are enforced by the Civil Nuclear Security and Safeguards (CNSS) section of ONR.

NISR 2003 (as amended) [14] places significant obligations on the operators of civil licensed nuclear sites relating to physical security measures for facilities, nuclear material and the security of SNI, ensuring that the prime responsibility for the implementation of arrangements for protection of NM, ORM, and associated facilities and SNI rests with the dutyholder.

During the GDA process, the principal applicability of NISR 2003 is in relation to the protection of SNI which may be generated or handled by the Requesting Party (RP) under Regulation 22. Compliance with these requirements of NISR during GDA is presented in Appendix A.

NISR 2003 also requires that all civil nuclear operators in the UK must produce and implement robust NSSPs. This will require that the plant has been designed to protect from the sabotage and theft of nuclear material and the theft of SNI and that adequate security arrangements are implemented on site to deliver this protection. In support of this, the GDA submissions including this GSR ensure that the generic methodologies and arrangements developed are suitable for future development into an NSSP by a future operator in accordance with NISR 2003, or to otherwise not foreclose NISR compliant options which a future operator may choose to implement.

3.4 ONR Guidance

The Security Assessment Principles (SyAPs) present ten Fundamental Security Principles (FSyPs) that define general security outcomes that the dutyholder must deliver. These FSyPs are either strategic enablers or are focused on the delivery of the security operations. Each of the FSyPs is supported by one or more Security Delivery Principles (SyDPs). The SyDPs support the dutyholder in the delivery of the FSyPs by presenting Relevant Good Practice

(RGP). Appendix D of this GSR presents these FSyPs and SyDPs and highlights how these are delivered by the SMR-300 project in GDA Step 2 for both Holtec Britain and Holtec International aspects of the project.

SyAPs also defines a set of seven Key Security Plan Principles (KSyPPs), which present the basis for an effective security plan and are applied across the FSyPs and SyDPs covered in a security plan. Where relevant to a Step 2 GDA assessment, these have been addressed by the underpinning philosophies and principles in Section 4.0 of this document.

The 2022 SyAPs [15] supported by protectively-marked Annexes (at Version 1.1), represent the extant document which is currently being used in all GDAs.

SyAPs provide ONR with a baseline against which to make regulatory judgements on the adequacy of security arrangements. In general, SyAPs reflect ONR's expectations for security submissions within a goal-setting and outcome-based framework and are benchmarked against international good practice and IAEA guidance. The SyAPs are themselves supported by Technical Assessment Guides (TAGs), and other guidance including Technical Inspection Guides (TIGs), to further assist decision making within the nuclear security regulatory assessment process.

Within the scope of this GDA, the following TAGs are particularly relevant:

- Categorisation for Theft (CNS-TAST-GD-6.1) [16].
- Categorisation for Sabotage (CNS-TAST-GD-6.2) [17].
- Physical Protection System Design (CNS-TAST-GD-6.3) [18].
- Protection of Nuclear Technology and Operations (CNS-TAST-GD-7.3) [19].
- Secure by Design (CNS-TAST-GD-11.4.1) [20].
- The Threat (CNS-TAST-GD-11.4.2) [21].
- Functional Categorisation and Classification of Security Structures, Systems and Components (CNS-TAST-GD-11.4.5) [22].
- Effective Cyber and Information Risk Management (CNS-TAST-GD-7.1) [23].
- Protection and Response to Cyber Security Incidents (CNS-TAST-GD-7.5) [24].
- Guidance on the Security Assessment of Generic New Nuclear Reactor Designs (NS-TAST-GD-11.1) [25].

ONR uses the SyAPs and TAGs to guide their regulatory judgements when undertaking assessments of security submissions. These will form the basis of ONR's judgement of the adequacy of the security case for the Generic SMR-300.

Although not all of SyAPs is directly applicable during the GDA process, the expectation is that the security arrangements detailed in this GSR will be suitable to meet regulatory expectations and be of value to a future licensee.

To facilitate the delivery of a graded approach to security, the SyAPs define a set of Physical Protection System (PPS) and Cyber Protection System (CPS) outcome and response effects together with indicative security postures within a series of protectively marked Annexes. The duty holder is required to meet the protection outcome and response effects but is given flexibility on how the outcomes and response effects are met provided that the security solution is justified. The Annexes also provide further details on the level of Unacceptable Radiological

Consequence (URC) to be considered in the security case as well as criteria for categorisation for theft and for Vital Areas.

3.4.1 Specific GDA Security Guidance

The principal source of guidance for a GDA security assessment is the Guidance on the Security Assessment of Generic New Nuclear Reactor Designs [25]. This TAG contains guidance to inform ONR inspectors in exercising their regulatory judgment during assessment activities related to the adequacy of generic designs for new nuclear reactors.

The ONR GDA Guidance to Requesting Parties [26] provides more general detail on ONR's expectations for the GDA process. This outlines a three-step approach for GDA, with the ultimate expectation (at the end of Step 3) for RPs to 'develop *a comprehensive generic security case, comprised of a GSR including relevant supporting reference documents'* which should '*describe the security features of the proposed design. It should document the categorisation from both theft and sabotage to determine the protective security outcomes and applicable security postures to be applied'*.

However, the GDA for the Generic SMR-300 is to conclude at Step 2. [26] states that '*For a GDA that completes at Step 2, ONR will provide a GDA Statement*' and it explains that '*there are a number of potential outputs that can be provided upon completing a GDA. The output provided will depend on the GDA scope agreed, the meaningfulness of the assessment undertaken, the adequacy of the safety and security cases submitted and the significance of any residual safety or security concerns that remain to be resolved*'.

Thus, Holtec's expectations are that the ONR GDA Step 2 statement would be consistent with the statements made at the end of Step 2 in previous GDAs, as defined by [26].

The sampling process in [26] highlights that *'…ONR focuses on, in broad terms…the overall design and safety and security claims, as well as the methodologies, approaches, codes, standards and philosophies during Step 2*', noting that this has been used to derive the scope presented in sub-section 5.1. [27] provides RGP for the security documents provided during a GDA. This is reflected by the security document structure used for GDA Steps 1 and 2, namely the development of the PSyR [1] in Step 1 which provided the outline of the GSR structure (and required supporting methodologies and analyses) which have been developed during GDA Step 2 (see subsection 1.4).

3.4.2 UK Relevant Good Practice

An expectation for the GDA is that the security submissions will draw upon RGP. In addition to examples of RGP outlined by ONR's TAGs and TIGs, other RGP has been identified from review of:

- Security submissions from current and previous GDAs, specifically for the Rolls-Royce Small Modular Reactor (RR SMR) and UK HPR1000 which were both regulated under SyAPs.
- ONR summary reports and feedback on the above.
- Information and guidance from industry bodies and associations such as National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC).

The security assessment methodologies developed by Holtec during GDA Step 2 identify and apply appropriate RGP from UK and international sources in areas such as Vital Area Identification, cyber security risk assessment and secure by design.

3.4.3 International Relevant Good Practice

In addition to international guidance identified earlier, RGP has been identified from security submissions to international regulators including, for example to the Canadian Nuclear Safety Commission (CNSC) Vendor Design Review (VDR) process which is a pre-licensing generic assessment analogous to a GDA.

In developing the SMR-300 GDA Step 2 GSR, Holtec has drawn upon, and learned lessons from, the development of security arrangements for the SMR-300 in United States (US), including feedback from the US Nuclear Regulatory Commission (NRC) licensing process.

4.0 SECURITY PHILOSOPHY AND PRINCIPLES

4.1 Introduction

This section outlines, at a high level, the philosophy and principles which have been applied to develop the GDA nuclear security assessments and this GSR. These have been influenced by consideration of KSyPPs 1, 3 and 4 [15], specifically **secure by design**, the **graded approach** and **defence in depth** respectively.

The security philosophy and principles underpin the development of the nuclear security case as it has evolved from the GDA Step 1 PSyR, to this Step 2 GSR and, ultimately, evolves into the NSSP.

4.2 Security Philosophy

A risk-informed, proportionate, and holistic approach has been followed to protect nuclear material and SNI[3] at an SMR-300 site through life which:

- Delivers security by design by seeking to integrate measures into the developing design rather than adding them later.
- Security-informs the design and layout of the plant from as early as possible in the design development (and modification) process.
- Integrates the security case with (in particular) the safety and safeguards cases.
- Incorporates an SbD hierarchy of risk controls (KSyPP 1).
- Is consequence-based to enable graded (proportionate) protective measures to deliver the security objectives (KSyPP 3).
- Recognises that whilst design and engineering is a key enabler to the management of security risk and delivery of the most effective means of risk control (see Figure 3), a robust security management system and culture are required during all stages of the project lifecycle to minimise the risk as shown in Figure 2 below.

[3] UK nuclear security legislation and regulation requires the protection of SNI at the site. However, this is outside the scope of the GDA as the presence and extent of SNI at a site are site-specific.

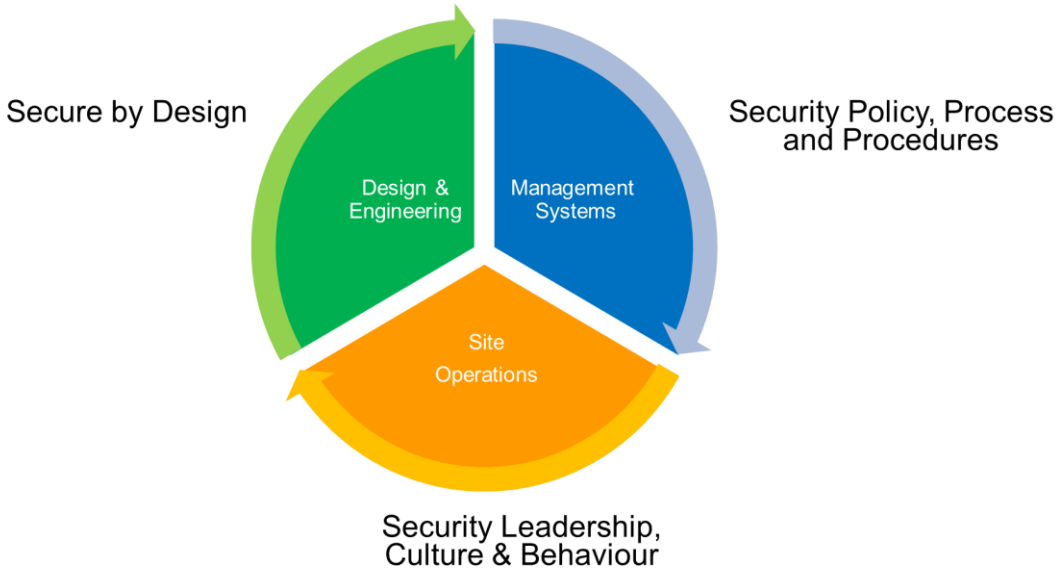

Figure 2: Security Risk Control Enablers

- Starts with the asset needing protection and adopts an 'inside-out' protection approach, which is more cost-effective and less resource intensive than the traditional approach of defending a facility from the 'outside-in', noting that the latter loses effectiveness with the ever-changing threat environment.
- Recognises that protection is provided via a holistic and integrated blend of physical, cyber and procedural measures which build on design and safety case robustness measures to provide defence in depth (KSyPP 4), rather than considering them as individual measures.
- Ensures that nuclear security arrangements will need to integrate seamlessly with the wider security and operational arrangements at the future site.
- Recognises that nuclear security is an enabler for safe and secure SMR-300 operations and not an inhibitor.

4.2.1 Secure by Design Principle

The SMR-300 security philosophy is influenced by KSyPP 1 and aims to deliver an inherently secure design by seeking to eliminate, or reduce, security vulnerabilities during the design process rather than addressing these later in the development lifecycle by retrospectively adding protective or mitigative security measures.

To support this aim, the SMR-300 Secure by Design Methodology [28] has been developed and adopted during GDA Step 2. This presents how the SbD principle is adopted in GDA Step 2 and beyond with the aim of eliminating, or minimising, the need for additional security controls at the site-specific design stage thereby simplifying security operations and reducing cost throughout the life of the plant.

This hierarchy is applied when considering key design decisions or assessing modifications to the plant during the GDA programme to ensure that the design is guided towards firstly 'designing out' security vulnerabilities or otherwise providing passive protection (e.g., plant

robustness) in preference to adding active security features such as access control or a response force. The secure by design principle can be illustrated by Figure 3 below:

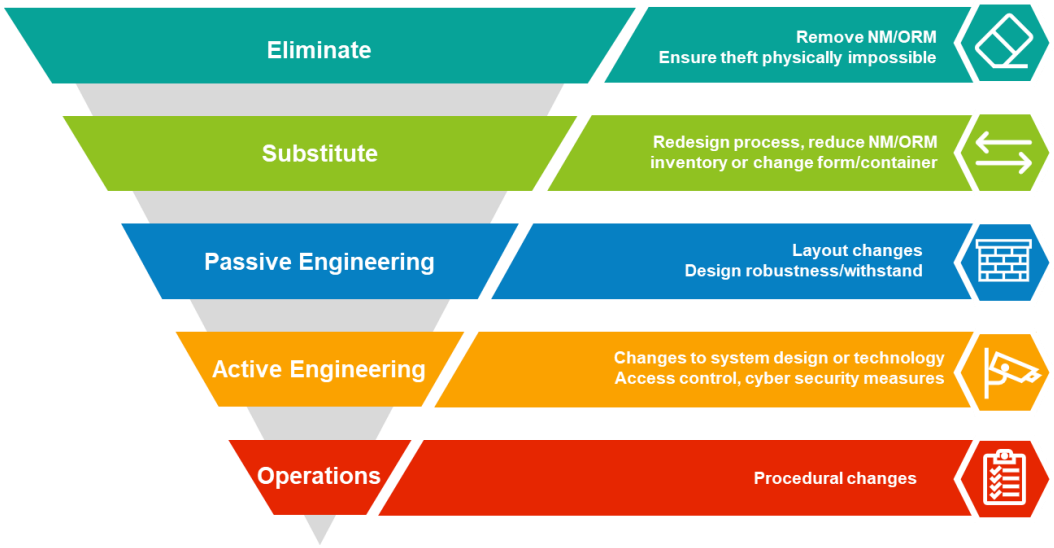

Figure 3: Secure by Design Hierarchy of Risk Controls

This hierarchy recognises that the most effective means of reducing security vulnerability and achieving an inherently secure design are through elimination of vulnerabilities, substitution of processes or through passive engineering. Furthermore, making appropriate design decisions provides for a long-term reduction in the capital and operational costs of providing physical security at the facility because of the reduction in the need for, and reliance on, protective security systems.

Figure 4 below highlights how the SbD Methodology applies to four different but complementary aspects as the project develops.

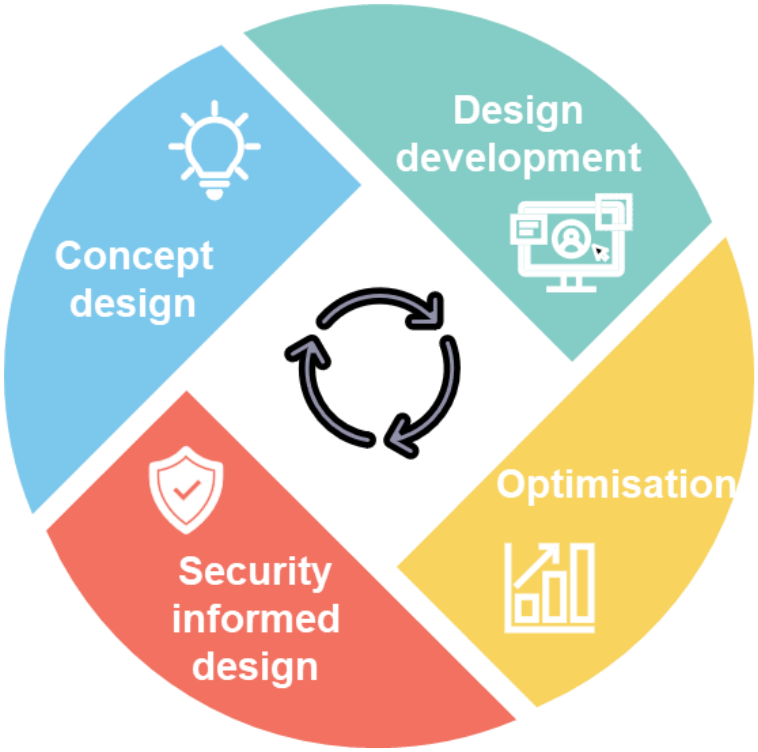

Figure 4: Elements of a Security by Design Approach

These four aspects of SbD defined by [28] can be summarised as:

- Concept design – reflecting that security-related considerations have been included in design choices adopted for the generic SMR-300 since project conception.
- Design development – as the design matures and specific assessments are undertaken (including those security risk assessments undertaken during GDA Step 2) these can be used to influence or propose modifications to the design from a security perspective.
- Security Informed design – as the design matures and further design decisions are made or modifications are proposed, the security discipline has visibility and influence over the design decision making.
- Optimisation – ensures that security is integrated with other disciplines and potential conflicts are addressed. This includes both physical aspects (such as evacuation route definition and the allocation of adequate space for security requirements) and organisational aspects (such as management systems and culture).

Hence, examples of how an SbD approach can eliminate or reduce security vulnerabilities include:

- Changes to the site and building layouts.
- Improving robustness of physical barriers (e.g., roofs, tunnels, walls, doors).
- Redundancy, separation, segregation and diversification of protective and mitigating systems.
- Identifying defensive cyber-security software/architecture measures.

Examples of more general SbD activities are associated with ensuring that the design can accommodate, and be influenced by, security requirements, such as:

- Ensuring space is available for security infrastructure (e.g., search areas, turnstiles, cabling and power supplies).
- Deconflicting safety and security requirements (such as emergency egress, alarm management and door functions).
- Review of proposed design modifications from a security viewpoint.

[28] defines how the Holtec Britain security team are involved in all these design activities, by providing advice on individual design activities, resolving conflicts between security requirements and other disciplines, participating in As Low as Reasonably Practicable (ALARP)/Optioneering studies or design review committees.

This is achieved through a regular and interactive process including the US-based design team and Holtec Britain Subject Matter Experts (SMEs) including:

- Security; specialists with expertise in security system design and programme implementation.
- Operations; over 150 years of licensed operational experience.
- Probabilistic Safety Analysis; system response to determine core damage releases.
- Civil/Structural Engineering; review Design Basis Threat (DBT) and Vital Area layouts to enforce design where needed to achieve safety objectives.
- System Design; review system responses to operations that could adversely impact core and spent fuel integrity.
- Instrumentation and Control (I&C)/Electrical; evaluate plant electrical and processing architecture for robustness from cyber and physical threats.

Details of how the SbD principle has been applied within the SMR-300 project to date are presented in subsection 5.2.7 which outlines how SbD has been applied in the design presented by the DRP [2] and subsection 7.7 which describes how SbD has been applied during the GDA.

4.2.2 Graded Approach

The application of the graded approach (KSyPP 3) ensures that the security assessments are undertaken commensurate with risk in order to ensure a proportionate assessment is undertaken and an appropriate security solution is developed. Specifically, the security risk assessment methodologies for the SMR-300 developed during GDA Step 2 [29] [30] [31] and outlined in Section 7.0 utilise consequence-based information to both determine the rigor and comprehensiveness of the assessments that are undertaken given also the availability of information at the particular stage of the project lifecycle.

Consequence-based information is used to apply an appropriate categorisation to the outputs of the security assessments (e.g. the categorisation of a Vital Area from sabotage, an area requiring protection of material from theft or potential effect of cyber-attack). These are used to determine appropriate security outcomes for the development of the design of the protection systems, with the highest categorisation categories requiring higher levels of protection. This

'golden thread' linking the outputs of the security risk assessments with the development of the protection system design is presented in [32] and outlined in subsection 7.5.3.

Similarly, Appendix A outlines how the development of arrangements by Holtec to comply with NISR Regulation 22 during the GDA process (and thereafter Regulations 4 to 12 and 22) have followed a graded approach according to the assessed risk as it changes as the project progresses through its lifecycle.

Furthermore, the graded approach is applied when considering the integration of security with other disciplines. The Secure by Design Methodology [28] outlines how the security discipline interacts with other project stakeholders when considering the suitability of proposed design modifications or for the resolution of conflicts between the requirements of separate disciplines. This approach contributes towards ensuring an overall 'balance' is achieved between security and other stakeholders, such as safety and safeguards, to achieve an optimised design for the SMR-300 for UK deployment, see also subsection 4.2.1.

4.2.3 Defence in Depth Principle

Defence in depth (KSyPP 4), or layered defence, is achieved primarily via an Integrated Security Solution (ISS) comprising multiple (independent or complementary) elements of security.

In many cases, security also benefits from defence in depth inherent in the safety design of the plant; for example, through the provision of multiple segregated trains of safety systems which would require an adversary to sabotage multiple locations in separate locations to achieve an aim of sabotaging a safety function. Similarly, robustness inherent in the design of the SMR-300 in areas such as radiation shielding and hazard protection can provide a security barrier.

The elements or layers of a defence in depth model take an inside out approach focused on the asset to be protected which is likely to be NM/ORM or an identified target within a safety system as illustrated in Figure 5. Robust defence in depth will take a comprehensive approach in order to provide a multi-layered and proportionate security against the full spectrum of security threats, to include physical, cyber and insider threats.

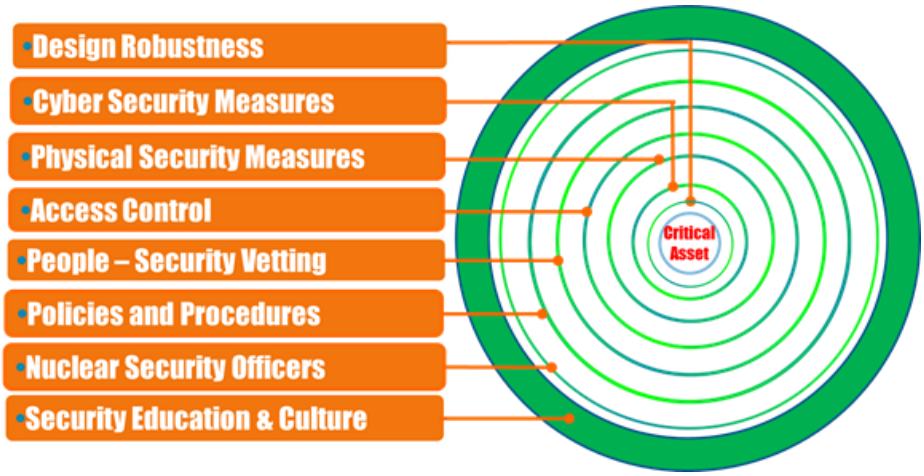

Figure 5: Defence in Depth

4.2.3.1 Integrated Security Solution

As highlighted in Figure 6, an ISS incorporates layers of measures associated with:

- Design and Engineering - Security informed design and its implementation.
- Management Systems – Policies, processes and procedures associated with the security design.
- Site operations - Security operations throughout the plant lifecycle from design, construction, and commissioning through operations to decommissioning.

Taken together, such measures provide a robust defence in depth security solution (in line with KSyPP 4). During GDA, the focus is on design and engineering aspects, in particular the application of the SbD principle to design-in robustness of the plant against potential sabotage or theft activities and the initial development of a concept of security operations which considers an outline of the physical protection architecture, infrastructure, and requirements at an early stage. Cyber security is also considered at this stage to ensure appropriate system architecture and interfaces can be defined which offer resilience to a cyber-attack.

This consideration is expanded to management systems and site operations as the project moves beyond GDA and into site licensing and is likely to include perimeter protection, security guarding and surveillance, noting the changing technological and threat environment.

The approach applied for the development of an ISS is outlined in the Conceptual Security Arrangements Report [32] and is discussed in subsection 7.5.3.

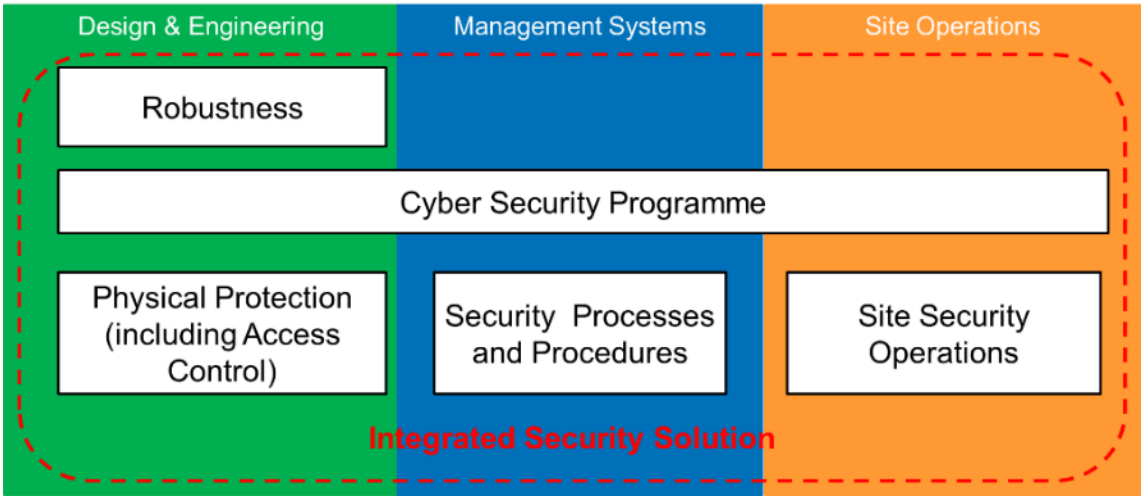

Figure 6: Integrated Security Solution

5.0 SCOPE OF GDA AND PLANT INFORMATION

5.1 Scope

The scope of the GDA is outlined in [3]. In line with this, the SSEC has been developed for a twin-unit reactor design to be constructed, operated, and decommissioned on a generic site that bounds all prospective sites considered within the SMR-300 Great Britain Generic Site Envelope (GB GSE).

5.2 Plant Information

5.2.1 Overview

An overview of the Generic SMR-300 is presented in [33] and summarised below.

The Generic SMR-300 is a 300 MWe (1,050 MWth) two-loop Pressurised Water Reactor (PWR) with forced circulation in normal operation, utilising two cold legs each with a vertically mounted reactor coolant pump, two hot legs, and a single once-through steam generator with an integral pressuriser stacked on top of the steam generator.

The SMR-300 safety systems are passive and are driven by natural forces (e.g., gravity, conductive and convective heat transfer), with no reliance on pumps, external water, or off-site power. Protected between a robust steel Containment Structure (CS) and a steel-concrete modular Containment Enclosure Structure (CES), the Annular Reservoir (AR) is the SMR-300's ultimate heat sink, containing a large volume of water surrounding the containment and providing passive cooling to the containment for at least thirty days in the case of a Design Basis Accident (DBA) by simple conduction and convection, followed by a transition to air cooling. No operator action is required to mitigate DBAs.

The SMR-300 employs an efficient reactor core design that contains a matrix of UO_2 fuel rods assembled into fuel assemblies along with control and structural elements. The reactor vessel internals support the reactor core, the control rod assemblies, and the control rod drive shafts. The internals channel the flow from the inlet nozzles (cold legs) through the core and to the outlet nozzles (hot legs). The fuel, reactor vessel internals, and coolant are contained within the Reactor Pressure Vessel (RPV). The SMR-300 uses a standard PWR fuel assembly and utilises Rod Cluster Control Assemblies (RCCAs) and soluble boron to control reactivity. The core is designed for a nominal 18-month cycle length with flexibility for longer or shorter cycles depending upon utility energy requirements.

After a postulated accident, such as a Loss of Coolant Accident (LOCA), the plant is designed to automatically achieve and maintain a safe shutdown state without need for operator action, external water, external power, and active systems.

The Generic SMR-300 has a compact plant arrangement, see Figure 7, which shows a conceptual layout plan for a twin unit power station. The SMR-300 plant site consists of the following principal structures:

- Containment Structure (CS).
- Containment Enclosure Structure (CES).
- Reactor Auxiliary Building (RAB).
- Intermediate Building (IB).
- Independent Spent Fuel Storage Installation (ISFSI).
- Annex Building.
- Turbine Building (TB).
- Diesel Generator Building.
- Waste heat cooling tower or HI-MAX Air-Cooled Condenser.

Structures within GDA scope and relevant to the nuclear security assessments at GDA Step 2 are discussed in the following sections.

Figure 7: Conceptual SMR-300 Layout

[REDACTED]

- [REDACTED]
- [REDACTED]
    - [REDACTED]
    - [REDACTED]
    - [REDACTED]
    - [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

5.2.2 Containment Structure

The CS is designed to remain intact and sealed during DBAs, [REDACTED] in the event of a DBA. The design incorporates highly reliable passive Engineered Safety Features (ESFs) along with an I&C system with multiple levels of anticipatory reactor trip signals. Defence in depth is provided via multiple and diverse simple pathways for heat rejection from the core.

[REDACTED]

[REDACTED]

5.2.3 Containment Enclosure Structure

The CES is a Seismic Category I structure that surrounds the CS and provides the following functions:

- Protects the CS from external hazards and threats.
- Provides shielding from radioactive sources inside the CS during power operations and postulated accidents.
- Forms the outer wall of the AR.
- Provides a vent for the AR to facilitate evaporative cooling.
- Interfaces with the IB, which protects the main steam and main feedwater lines until their respective safety isolations and seismic restraints. The CES provides support for these lines at the CS penetration.

[REDACTED]

5.2.4 Reactor Auxiliary Building

The RAB is a seismic Category I structure and is adjacent to the CES. [REDACTED]. The Radiologically Controlled Area (RCA) contains systems to support normal primary plant operations.

[REDACTED] The major equipment, systems, and functions contained within the RCA are:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

Within the RCA, the FHA services both units and has the following functional areas:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED] New fuel is transferred in a HI-TRAC within a Multi-Purpose Canister (MPC) which comprises a fully welded stainless steel canister providing a safe containment of SMR-300 spent fuel for on-site transfer and storage. [REDACTED]

[REDACTED]

[REDACTED]

5.2.5 Intermediate Building

[REDACTED]

5.2.6 Dry Fuel Storage

[REDACTED]

The VVM, akin to an aboveground overpack, is comprised of a cavity enclosure container and closure lid, as well as interfacing structures. The MPC is a fully welded stainless steel canister providing a safe containment of SMR-300 spent fuel onsite or for offsite transport. It utilises a honey-comb fuel basket comprised of Holtec's proprietary material Metamic HT™ to provide positions and reactivity control for SMR-300 fuel assembles.

Each MPC provides sufficient capacity (with margin) to transport the nominal core batch size of new fuel during refueling and discharge spent fuel for [REDACTED].The HI-TRAC is a steel, lead, and water-shielded transfer cask which houses the MPC during onsite transfer prior to placing in the UMAX. It provides shielding to workers during loading operations and protects the MPC from DBAs.

[REDACTED]

5.2.7 Secure by Design Considerations

The development of the design of the Generic SMR-300 to the DRP declared during GDA Step 2 [2] has incorporated the principle of SbD and the associated hierarchy of controls (see sub-section 4.2.1 and Figure 3). This is outlined within subsection 7.7 and in more detail in [34]. Key SbD decisions made in the development of the DRP design [2] are summarised below.

The Generic SMR-300 has a small nuclear island footprint and a lower radiological inventory when compared to standard larger PWRs. The design philosophy provides a number of passive safety systems [REDACTED]. This provides protection against an external assault without reliance on external supporting systems which also has the effect of reducing [REDACTED].

[REDACTED]. The fuel import and export process utilises a highly robust and proven proprietary Holtec cask system which provides significant protection against sabotage and theft.

[REDACTED]

6.0 NUCLEAR SECURITY CASE

6.1 Introduction

In line with the security philosophy and principles (subsection 4.2), nuclear security for the SMR-300 plant is delivered via the following series of activities which, taken together, provide a structured, clear, and logical approach to the development of the conceptual security arrangements for the SMR-300.

The key steps of this approach are:

1. The nuclear inventory comprising NM and ORM at the SMR-300 facility is identified.
2. The SNI[4] on the SMR-300 site is identified.
3. An appropriate threat is used to define the physical and cyber threat at the SMR-300 site and is regularly reviewed to accommodate developments in the threat and understand certain credible beyond DBT scenarios.
4. The assets and areas within the SMR-300 facility requiring protection to prevent the sabotage of the nuclear material inventory are identified, and any Vital Areas are categorised.
5. The assets and areas requiring protection to prevent the theft[5] of the NM/ORM or SNI are identified (including categorisation for theft of NM/ORM).
6. Protection against sabotage and theft is provided by a blend of protective physical, cyber and procedural measures to provide defence in depth.
7. Areas within the nuclear facility are security zoned to facilitate the provision of graded protection, which is delivered by an ISS.
8. The site security operations deliver the ISS, which is regularly tested and reviewed to confirm its ongoing validity and effectiveness during the plant lifecycle, within an effective security culture.

These activities are illustrated in Figure 8 and form the basis for the development of this GSR. To present an overall and integrated picture, the need to identify and protect safeguards systems is included in Figure 8, noting that the provision of safeguards systems is addressed by the PSgR [4].

Other assets of importance to nuclear safety (e.g., emergency response systems and equipment) may require protection from sabotage. However, these are not within the scope of the GSR but will be considered post-GDA during the development of the site-specific security arrangements.

The identification of SNI is represented in Figure 8 for completeness and will be assessed during future site-specific assessments (see also Appendix A.4).

[4] Whilst site-based SNI does not form part of the GDA scope it is included here for completeness.
[5] Theft of NM by the nation state is covered by the nuclear safeguards case for the SMR-300 (see [4]), which is not covered by the SMR-300 nuclear security case.

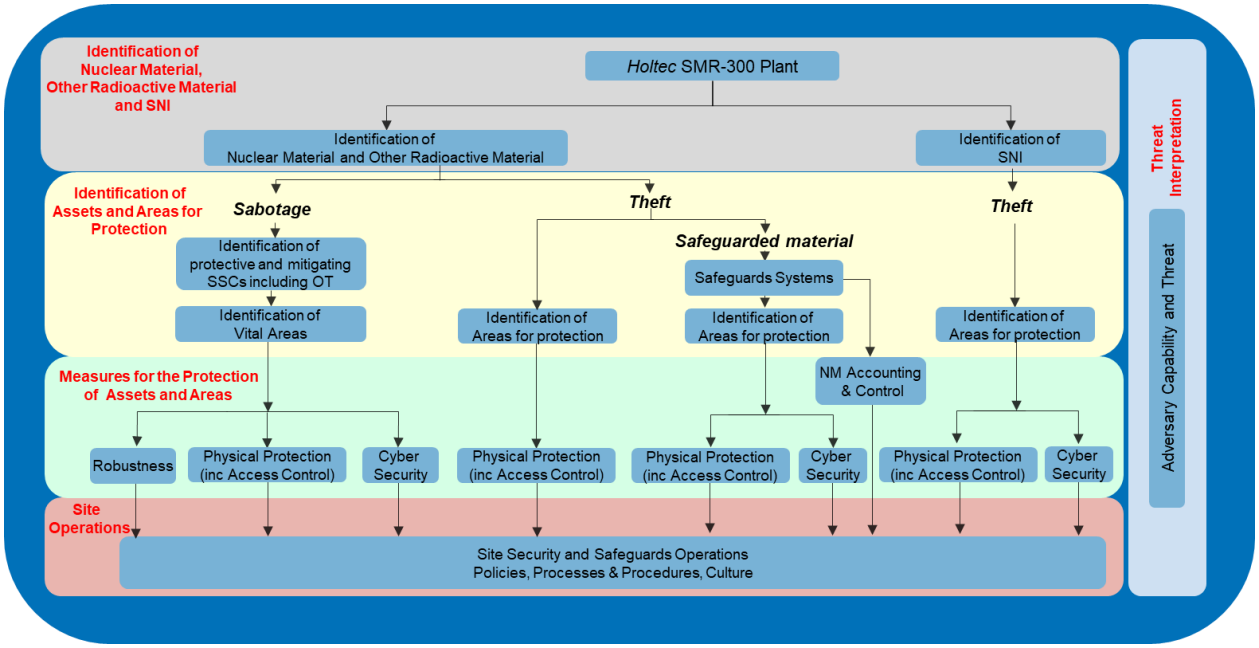

Figure 8: Delivery of Nuclear Security for the SMR-300

6.2 Security Claims

The Nuclear Security Fundamental Objective forms one of four fundamental objectives which are decomposed from the SSEC Fundamental Purpose (sub-section 1.2). This identifies that *security risks are managed to protect workers and the public from a radiological event arising from the theft or sabotage of nuclear or radioactive material (or supporting systems), or through the compromise of SNI.*

This aim is supported by seven high-level Security Claims (SyCs) which are delivered by the SMR-300 nuclear security case and, ultimately, to the NSSP (see Figure 9 below). These claims reflect the structured delivery approach outlined in Figure 8.

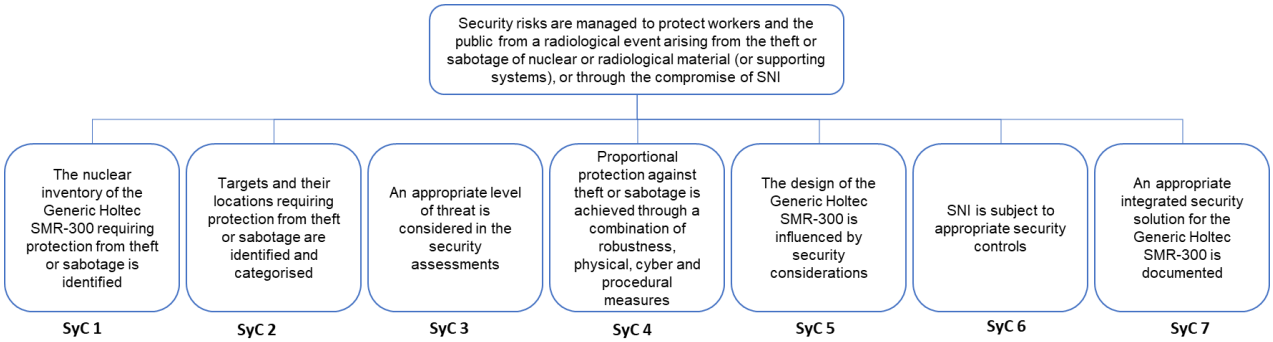

Figure 9: SMR-300 Security Case Aim and High-Level SyCs

6.3 Security Sub-Claims

During GDA Step 2, these seven SyCs have been decomposed, where necessary, into further sub-claims in alignment with the Claims, Argument, Evidence (CAE) derivation approach

outlined in PSR Part A Chapter 3. The security-specific claims and sub-claims are integrated into the overall SSEC CAE structure [35] and are presented in Appendix B.

Appendix B includes a mapping of the security claims to the relevant sections of this document to provide a route map of how the GSR addresses these high level claims. Appendix B also highlights how the GSR document structure (as presented in Figure 1) addresses the security sub-claims and argument and evidence level.

6.4 Integration with the Safety, Environmental and Safeguards Case

The SMR-300 GSR integrates with the SMR-300 SSEC via the SMR-300 Fundamental Purpose [36] as illustrated below.

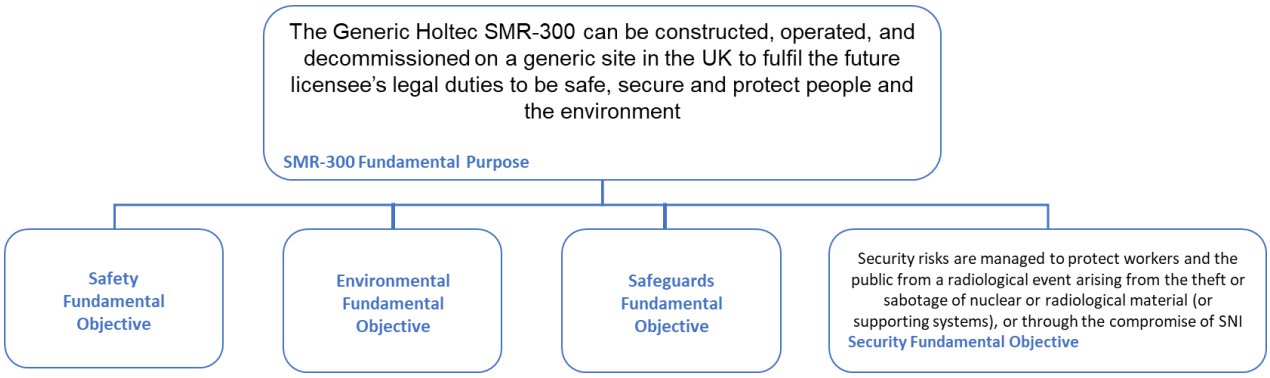

Figure 10: Integration of the Security Case with the SSEC

6.5 Security Design Principles

The Generic SMR-300 design has been developed by Holtec International to the current DRP [2]. For security aspects, the design development has been in accordance with the SMR-160 Design Standards for Security and Safeguards [37].

As no UK-specific design has been developed during GDA Step 2, it has not been appropriate to develop UK-specific security design principles at this stage. However, post-GDA a future licensee may decide to develop their own security design principles to support the implementation of SyC 5 (Security-influenced Design) during the design process, in line with [38], including to:

- Provide an aid to design decision making.
- Reduce or eliminate the requirement for physical and cyber-protection systems to be required, with consequent reduction in lifetime operational costs.
- Enable integration with nuclear safety and environmental approaches.
- Provide a 'golden thread' for demonstration of design optimisation.

The interface of the SbD process with design development is outlined in [28].

7.0 DELIVERY OF SECURITY

7.1 Introduction

As has been described throughout this document a security risk-informed and asset-focussed approach has been taken to develop a set of nuclear security arrangements which:

- Are inherently **iterative** and will develop according to the threat environment, assets that require protection and the stage of SMR-300 deployment to support the future licensee.
- Demonstrates the **Defence in Depth** principle which takes a comprehensive and layered approach in order to provide robust defence against physical, cyber and insider threats.
- Incorporates the **Secure by Design** principle to design out security risk at the earliest stage in order to simplify future security operations and reduce operational costs.
- Are **proportionate** to the security threat in order to support both secure and efficient nuclear site operations.

A security risk-informed approach (supported by the appropriate security governance framework) ensures security risks are identified, recorded, reviewed and managed. Ideally security risks will be eliminated (Secure by Design) or managed to a point where residual risk is within risk appetite. Where this is not possible security risks will be mitigated with appropriate, effective and proportionate control measures which will be developed in the post-GDA stages of security planning.

The approach follows a consequence-based and asset-focused approach which begins with the asset requiring protection from sabotage and/or theft, which for this assessment is the NM/ORM located at the Generic SMR-300 site. A comprehensive design and safety-informed process is applied which is based on an understanding of how the Generic SMR-300 may be sabotaged either through a physical or cyber-attack (or a combination of both as a blended attack) and the potential consequences, or be subject to theft/removal of NM/ORM.

Those measures in place which prevent the adversary from achieving their objective are identified and compared with the capability and capacity of the threat to confirm if the identified sabotage and theft scenarios are credible. [REDACTED].

The output of this process is a security-informed design with graded protection which will form the basis for a future operator to consider within the development of their NSSP.

The assessments undertaken in GDA Step 2 are based on information available at the time of assessment and will need to be reviewed, revised and/or extended by further assessments as the design matures and site-specific aspects are introduced.

The ‘golden thread’ that links this information and assessments together through the whole of the security case is illustrated in Appendix F.

7.2 Identification of Nuclear Material, Other Radioactive Material and Sensitive Nuclear Information

The most significant nuclear security related risks which are considered during the GDA are:

- [REDACTED]

Therefore, and in line with an asset-focused approach, the starting point for the nuclear security case is the [REDACTED] for the nuclear plant, as the primary aim of the GDA security case is to protect the NM/ORM from theft or sabotage. [REDACTED].

[REDACTED]

7.3 Identification of Assets and Areas for Protection

7.3.1 Introduction

[REDACTED]

7.3.2 Sabotage

7.3.2.1 Introduction

Sabotage of the generic SMR-300 is assessed through the application of a VAI&C methodology. A Vital Area is defined by ONR as '*an area containing NM/ORM, or equipment, systems, structures or devices, the sabotage or failure of which, alone or in combination, through malevolent acts, could directly or indirectly result in a URC, thereby endangering people and the environment by exposure to radiation'* [15].

The SMR-300 VAI&C methodology [31] has been developed by Holtec Britain during GDA Step 2 and considers:

- Identification, properties and locations of NM and ORM with potential to create a URC if sabotaged.
- Identification of events, or combinations of events, which could lead to a URC.
- Identification of potential Targets (SSCs, and their supporting systems where appropriate) which would require sabotage for a URC to be created either alone or in combination with sabotage of other areas of the SMR-300 facility.
- Locations of Targets.
- Mapping of threat information (see sub-section 7.4) to determine credibility.
- Identification of Vital Areas.
- Categorisation of Vital Areas based on the magnitude of the potential radiological consequences of sabotage based on Annex B of [15].
- A review process for updates or changes to the assessment.

The overall VAI&C Methodology comprises four distinct phases and is presented in Figure 11 below.

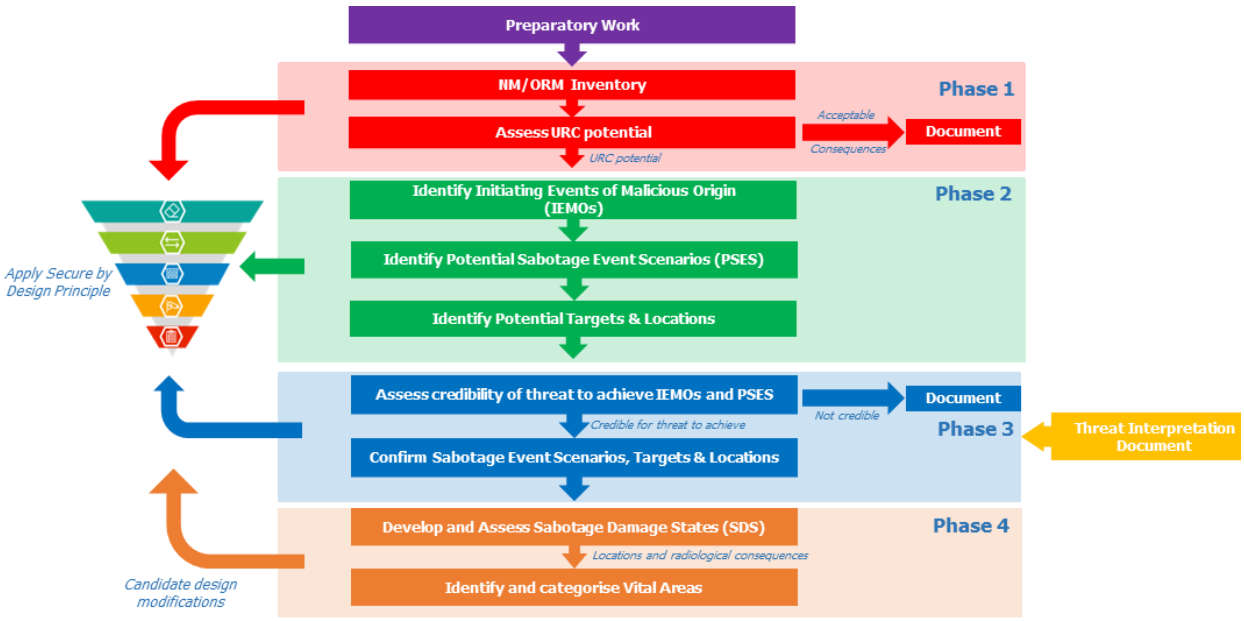

Figure 11: SMR-300 Vital Area Identification and Categorisation Methodology

[REDACTED]

As noted in subsection 7.2, the NM/ORM inventory was derived as part of the VAI&C Study and agreed with a multi-disciplinary group of stakeholders who attended the Vital Area Identification workshop.

7.3.2.2 Phases 1 & 2

[REDACTED]

The individual combinations of sabotage events which could lead to a URC are termed as Potential Sabotage Event Scenarios (PSESs). [REDACTED].

The SLM utilised the information from the sabotage FMEAs as well as safety case assessments (including the preliminary fault schedule and accident progression event trees from the [REDACTED].The progression of an IEMO to a URC was mapped using event trees. Top events in the model were developed into fault trees which considered the sabotage of individual target systems, including their supporting and interfacing systems as applicable. In this way, all potential combinations of sabotage events based on the model logic could be obtained, noting that a sabotage event could model a physical attack, a cyber-attack, malicious insider action or a direct attack using capabilities defined by the defined threat. Hence PSESs generated in this way automatically combine such events as appropriate into PSESs which represent ‘blended attacks’. The development of the SLM is represented in Figure 12.

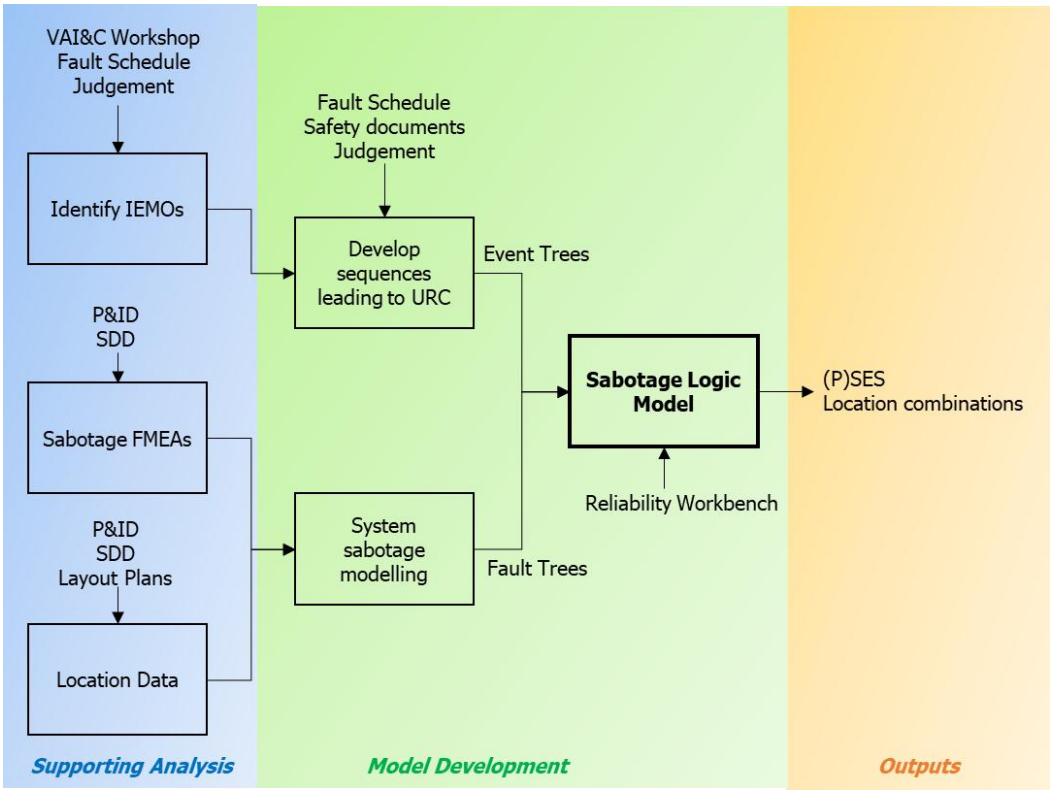

Figure 12: Sabotage Logic Model

[REDACTED]

7.3.2.3 Phase 3

Phase 3 of the VAI&C study comprised a high-level threat application which applied professional judgement to assess each PSES against the assessment steps outlined in the VAI&C methodology. This use of professional judgement is appropriate given the level of design details (such as plant layout, pathways and structural robustness) available at the time of the assessment. For each PSES it was judged whether the PSES can be ruled out based on [REDACTED].

[REDACTED]

[REDACTED]

7.3.2.4 Phase 4

[REDACTED]

[REDACTED]

As highlighted in Figure 11, each phase of the VAI&C Methodology provides an opportunity to identify SbD options which could be used to eliminate or otherwise reduce the sabotage risk based on the hierarchy of controls presented in Figure 3. [REDACTED].

7.3.2.5 Judgement-based Vital Area Identification

The JBVAI (reported in Appendix E of [39]) presents the findings of a simplified desktop approach comprising a review of available information which used judgement to identify potential candidate Vital Areas across the generic SMR-300 at an early stage of GDA Step 2. [REDACTED].

7.3.3 Theft

The SMR-300 Theft Methodology and Analysis Report [30] presents the methodology and assessment applied to the categorisation for theft during GDA Step 2. This provides a graded approach to categorisation, in line with [REDACTED].

For the SMR-300, NM is expected to be limited to:

[REDACTED]

7.4 Threat Information

7.4.1 Introduction

The use of appropriate threat information underpins the security risk assessments, the design of both the plant itself and the security systems. A proportionate and evolutionary approach has been applied for the use of threat information during the SMR-300 project as illustrated in Figure 13 below.

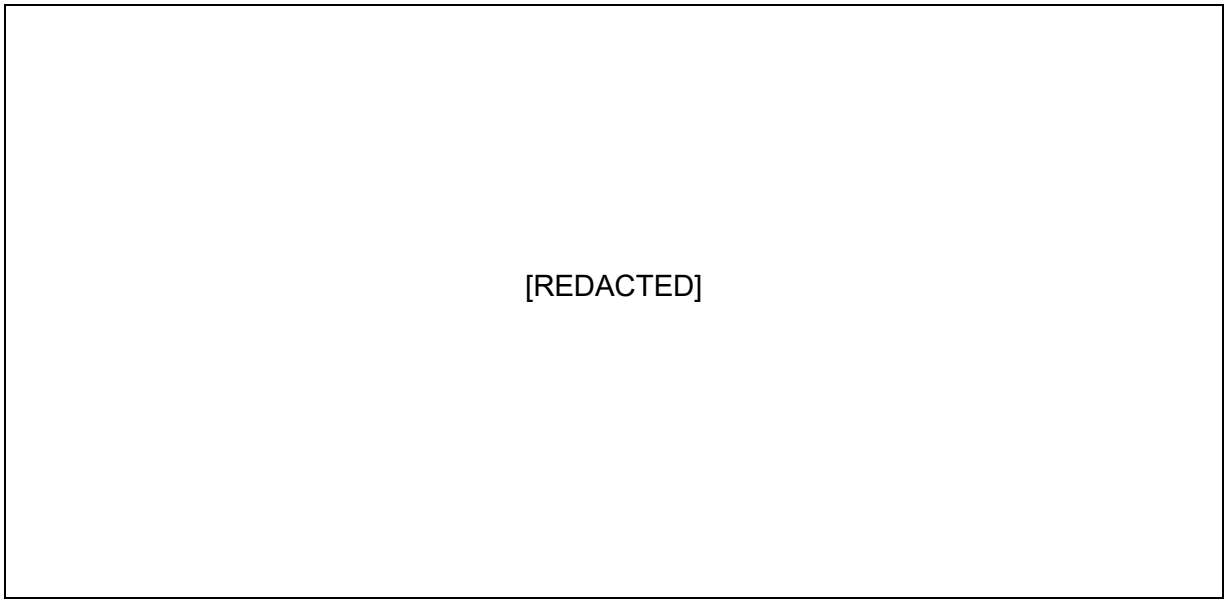

Figure 13: Evolutionary Use of Threat in SMR-300 Security Assessments

Figure 13 highlights how, during development of the Generic SMR-300 design up to the declared DRP [2], a robust security design to protect against the US DBT has been developed which gives confidence that the SMR-300 will be shown to be compliant with NISR which ultimately requires protection against the UK DBT.

During GDA Step 2, the security assessment demonstration studies, including vital area identification and cyber-security risk assessments, provide further confidence that the SMR-300

security design can be shown to be compliant with NISR and also provide an early opportunity for the identification of any UK-specific security design challenges to the generic SMR-300 design in line with the SbD principle. For these studies, a GDA Step 2 threat has been developed and applied as outlined in sub-section 7.4.2 below. The rationale for adopting this approach is outlined further in [34].

After GDA Step 2, future security assessments and a UK-specific design will be developed to protect against the UK DBT [40] which has been identified as a GDA Security Undertaking, see subsection 7.8. The UK DBT is determined by the UK government and stems from an 'intelligent adversary' who acts in a deliberate, planned fashion. The UK DBT is issued periodically by the Department for Energy Security & Net Zero (DESNZ) and is based around threat assessments undertaken by several lead government departments and agencies.

7.4.2 GDA Step 2 Threat

During GDA Step 2, a methodology for the development of an appropriate threat has been developed which outlines how suitable threat information can be derived from publicly available information, as summarised in Figure 14 below.

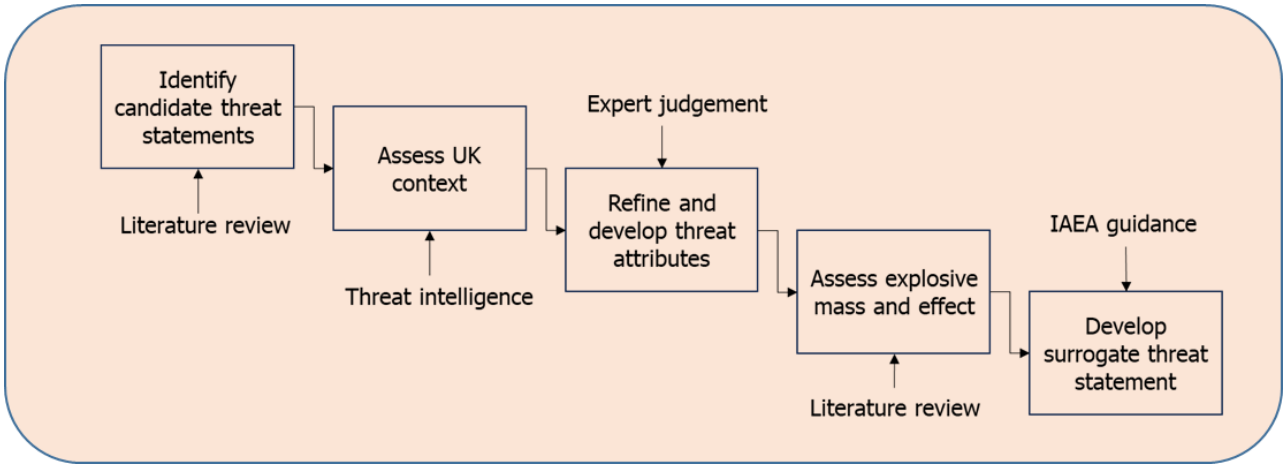

Figure 14: GDA Step 2 Threat Development Methodology

This approach is founded on a comprehensive literature review of publicly available information to identify contemporary information upon which to base the various methodology steps to develop the GDA Step 2 threat. This included:

- Development of an outline of a potential adversary threat capability for the sabotage or theft of material from a nuclear site.
    - To support this, a search was undertaken for unclassified DBT statements provided by different nation states.
- Review of current threat information for the UK to ensure that the unclassified DBT statements were applicable to the UK context.
    - This provided further information on approach, aim, motivation and organisation of potential adversary groups in the UK.

This enabled a refined threat to be developed which derived the attributes of the potential adversary group in terms of:

- Numbers of assailants.
- Skills.
- Weapons and equipment.
- Potential attack types.
- Size and effect of explosive devices.
- Role of insider(s).

For cyber threats, the threat document derived the attributes of the potential adversary group in terms of:

- Threat Actor.
- Threat Actor intent and capability [8].
- The use of an insider either within the Nuclear Site or within the supply chain or other trusted third parties.

[41] presents a threat statement which summarises the analysis undertaken into a clear and easily applied format in line with IAEA threat statement guidance [42].

7.5 Protection of Assets and Vital Areas

7.5.1 Introduction

Having identified the assets and areas requiring protection from sabotage and theft (subsection 7.3) and established the adversarial threat and capability (subsection 7.4), protection needs to be provided to ensure that the security fundamental objectives are delivered.

The protection is provided via an ISS for the plant. The ISS comprises a blend of robustness in design, physical and cyber protection measures, and the on-site nuclear/off-site response force capability, as required by category of nuclear material on-site. The development of the protection measures is based on the key philosophies outlined in Section 4.0.

During GDA Step 2, the development of an appropriate and graded set of physical, cyber and access control measures has been demonstrated based on the security risk assessments undertaken during GDA Step 2. This section outlines the approach taken to derive a representative suite of generic security arrangements for the SMR-300 to achieve the required Security Outcomes in line with [15].

7.5.2 Cyber Security Risk Assessment

During GDA Step 2, a SMR-300 CSRA methodology [29], has been developed, tested and applied through an initial study undertaken to demonstrate its use [43].

[REDACTED]

7.5.2.1 Cyber Security Risk Assessment Methodology

The SMR-300 CSRA methodology can be applied to both CBSIS, typically operational technology, and Computer Based Security Systems (CBSy). It is derived from International

Standards and RGP, specifically IEC 62645 [44] and the supporting standard IEC 63096 [45] and is in accordance with the guidance provided within SyAPs [15].

The methodology includes the following aspects:

- Assignment of Security Degrees (SD) to systems based on safety consequence.
- Assignment of CPS Outcomes to systems based on system consequences and threat information.
- Screening risk assessment for low consequence systems.
- Detailed cyber-security risk assessment of safety significant systems including assigning risk levels and determining if CPS outcomes are achieved.
- Guidance on the assignment of control sets to security risks/systems based on system SD.
- A methodology for assessing security risks across multiple I&C systems.

The cyber-security risk assessment methodology for single CBSIS is presented within Figure 15.

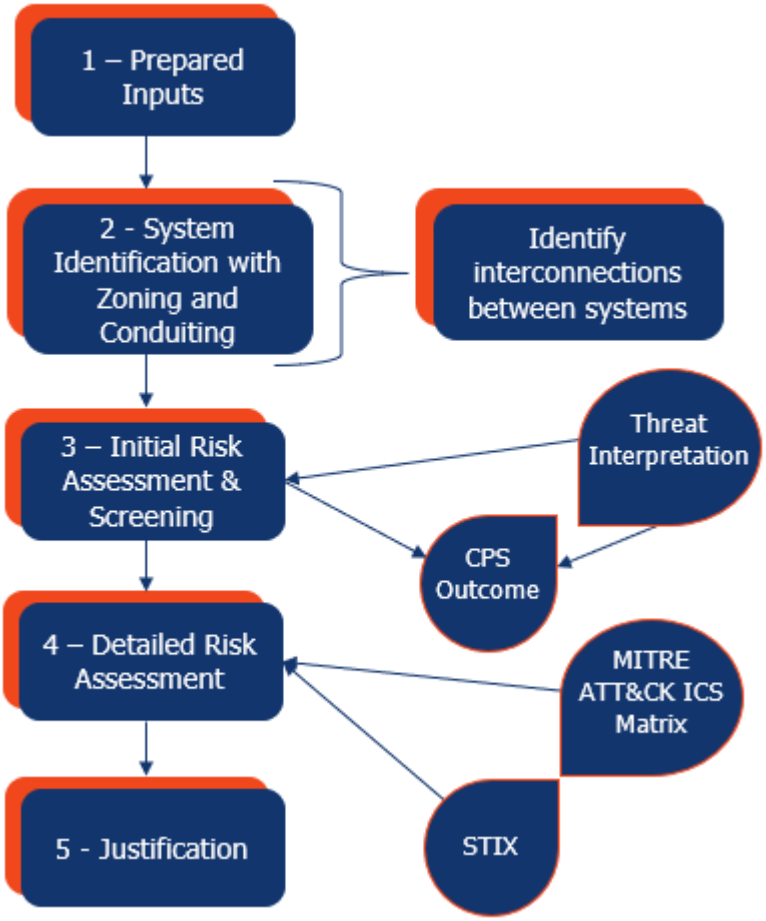

Figure 15: Overview of Cyber Security Risk Assessment Methodology for Single Systems

[REDACTED]

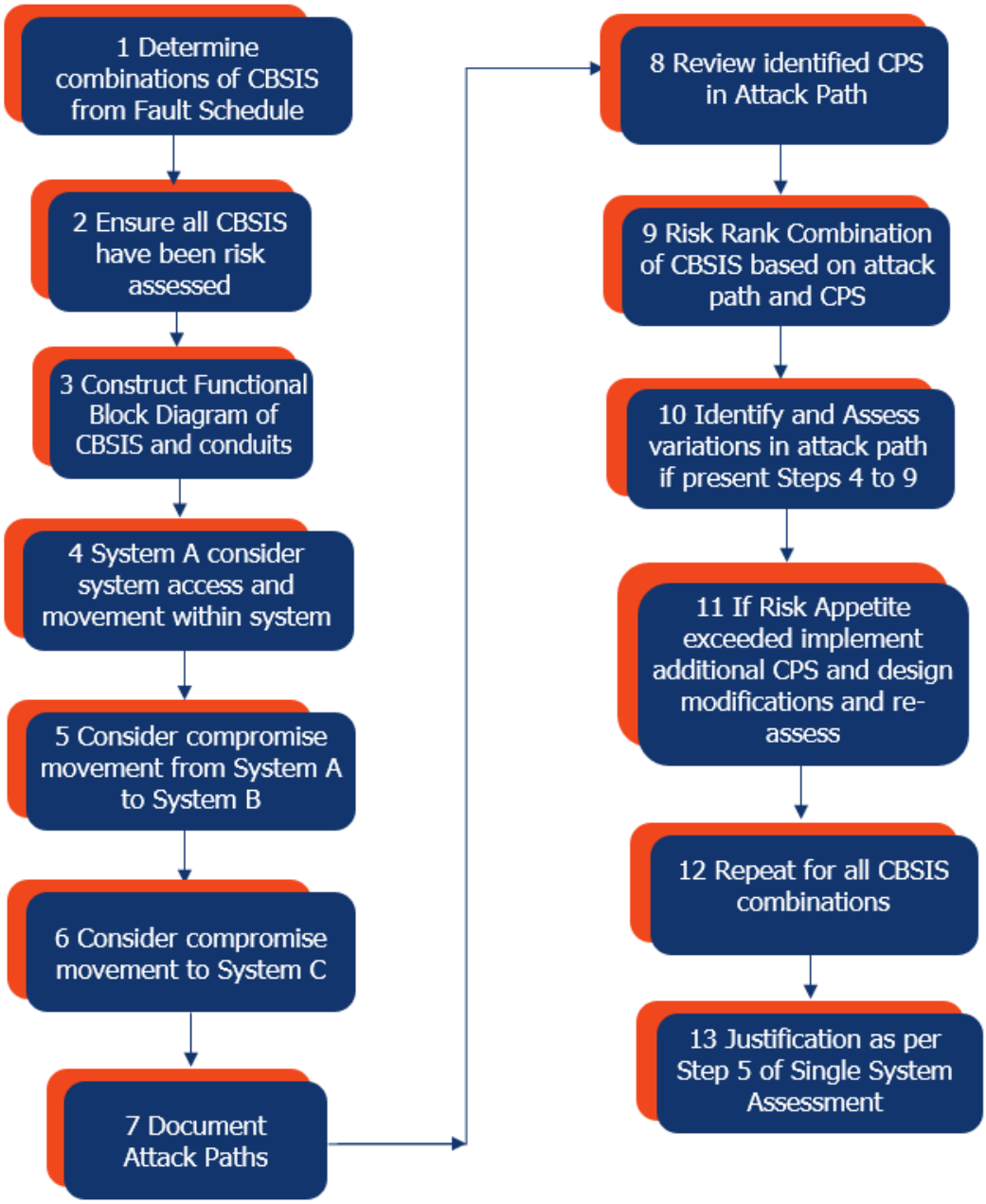

Figure 16: Multi-System Justification Methodology

The outputs of the CSRA are:

[REDACTED]

7.5.2.2 Cyber Security Risk Assessment

In GDA Step 2, the CSRA Study Report [43] presents the implementation of the CSRA methodology to undertake a cyber security risk assessment of the Generic SMR-300 PSS.

The CSRA of the PSS presents credible Threat Actors, and cyber-attack methods to derive cyber risks, provides an unmitigated risk ranking and the CPS outcome. Control Sets are identified and mitigated risks taking into account the identified Control Sets are also provided.

Where the mitigated risk is higher than the acceptable risk appetite, then the following mitigation measures were identified:

- Provision of additional Control Sets.
- Identification of design change recommendations (to be evaluated via the Secure by Design process).

[REDACTED]

7.5.3 Conceptual Security Arrangements

7.5.3.1 Introduction

The outputs of the VAI&C [39], Theft [30] and CSRA [43] assessments form a key input into the development of the required security architecture and infrastructure for the generic security arrangements to protect the SMR-300.

The Conceptual Security Arrangements (CSA) Report [32] provides a framework for the development of graded and integrated security arrangements which, together, can:

- Deliver a proportionate defence in depth security regime.
- Meet the required PPS and CPS outcomes under Annex C, D, and E of [15].
- Protect the NM/ORM from sabotage or theft.

[32] presents a high-level overview of how the residual security risk at the Generic UK SMR-300 will be managed through the provision of the Security Architecture (SA), Security Infrastructure (SI) and an appropriate Concept of Security Operations (CONOP). In GDA Step 2 this is in the form of an overview which is commensurate with the current level of design development and security assessment undertaken. However, this can form the basis for the future development of an ISS in support of the development of a site-specific security plan for the UK deployment of the SMR-300.

Hence, [32] presents a framework for the:

- Definition of the degrees of security that will be required at an SMR-300 in the UK in order to deliver the appropriate levels of protection; the SA.
- Identification of the layers of security measures, both physical and cyber, which can be used to provide a graded ISS at the levels defined in the SA at an SMR-300 in the UK; this together with the supporting services to the security systems, such as power supplies; the SI.

- CONOPs, i.e. the management of the security systems, for example monitoring of alarms and alerts and the delivery of the overall security arrangements at an SMR-300 in the UK.
- Development of a suitable NSSP post-GDA Step 2; Appendix E of [32] contains a suggested list of topics for a future NSSP to include.

Hence, the aim of employing SA and SI is to deliver graded security to protect:

- Vital Areas from sabotage.
- NM/ORM from theft.
- Safeguards equipment.
- Security equipment.
- Emergency response equipment.
- SNI from theft or manipulation.

This will be achieved by:

- Preventing unauthorised access to Vital Areas.
- Preventing unauthorised removal of NM/ORM.
- Protecting CBSIS and CBSy from sabotage.
- Protecting security equipment other than CBSy and emergency equipment from sabotage.
- Protecting Nuclear Material Accounting and Control (NMAC) and other safeguards equipment.
- Protecting SNI from theft or manipulation.
- Implementing a range of counter-insider measures.

7.5.3.2 Approach

To select appropriate PPS and CPS that will protect assets from theft and sabotage whilst allowing the SMR-300 to operate, it is necessary to:

- Determine which assets need to be protected.
- Identify where those assets are located.
- Determine the appropriate levels of security to be applied and
- Define an ISS for the SMR-300 for UK deployment.

Figure 17 outlines how the CSA has been developed during Step 2 of the GDA. This illustrates the ‘golden thread’ that links the security assessments undertaken during GDA with the development of illustrative SA, SI and a CONOP framework which feeds into the NSSP.

This golden thread shows how:

- NM/ORM is identified.
- Assets requiring protection are identified.
- Physical and cyber barriers and other protective security measures are established to protect the assets against sabotage and theft.
- Physical barriers, protective security measures and cyber security measures together with the provision of ‘defence in depth’ and proportionality are provided (via examples).

During GDA the intention is to provide a suitable framework and illustration of an approach to developing appropriate security arrangements for a UK-based SMR-300 power station. Hence, this approach identifies expectations and commitments for a future licensee to consider or adopt without precluding their ability to define their own suitable arrangements.

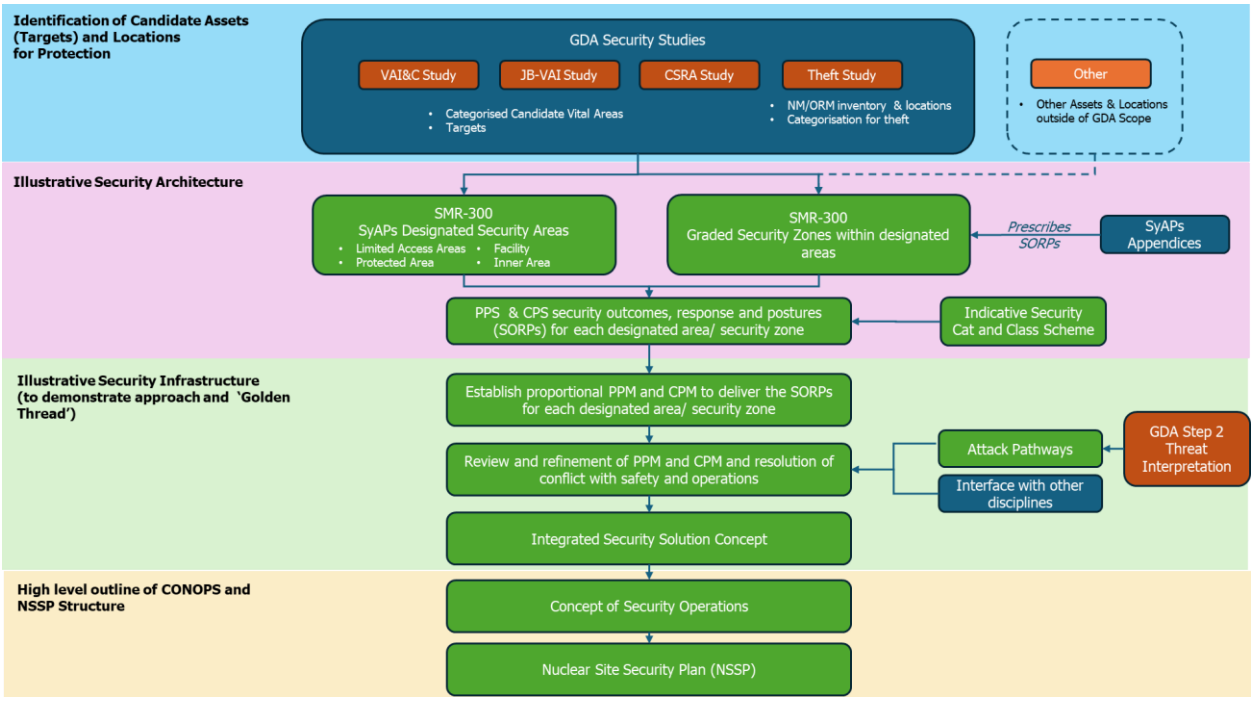

Figure 17: Development of Conceptual Security Arrangements during GDA

7.5.3.3 Security Architecture

The development of the SA for the SMR-300 during GDA (including the link to input studies) is illustrated in Figure 18.

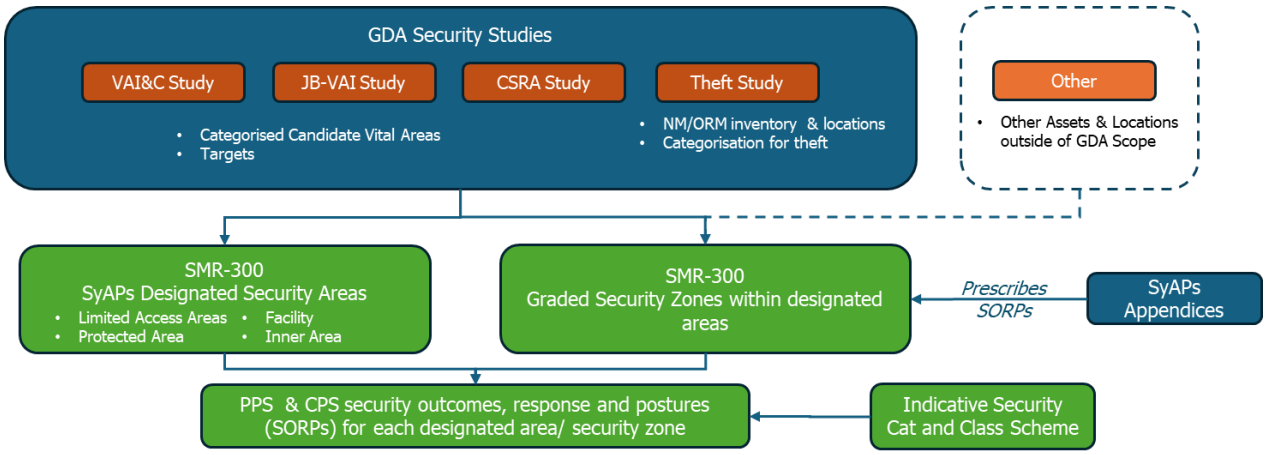

Figure 18: Development of Security Architecture in GDA

[32] presents an example of how the Generic SMR-300 site defined in [2] could be divided into Designated Areas based on the outputs of the security risk assessments undertaken in GDA Step 2. For each facility identified as containing Vital Areas or areas requiring protection from theft of NM/ORM, a bounding PPS outcome[6] was determined.

The following Designated Area types were defined in [32]:

- Limited Access Area
  - An area to which access is limited and controlled for physical protection purposes. It comprises the external boundary to the site and is hence part of the site-specific design and hence is addressed only at a conceptual level in GDA Step 2.
- Protected Area
  - An area contained within the Limited Access Area and forms a second layer of security for the protection of HCVAs and quantities of Category I and II Nuclear Material.
- Facility
  - A facility is a building in which NM/ORM is produced, processed, used, handled, stored or disposed of. The facility provides a third layer of security.
- Inner Area
  - Required specifically where Category I quantities of NM are used or stored. Material of this category is not identified within the NM for the Generic SMR-300 hence Inner Areas are not considered further in GDA Step 2.

[REDACTED]

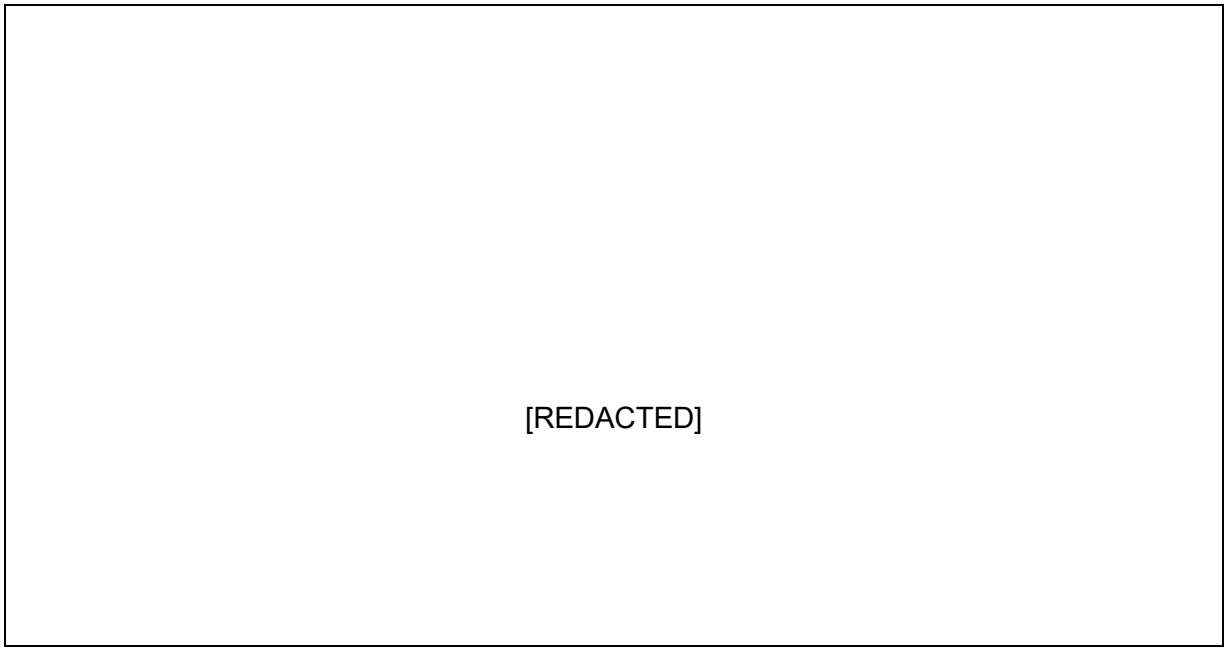

Figure 19: Generic SMR-300 Designated Areas (Example)

[6] Representing the most onerous outcome required within the facility.

In addition, four security zone types were proposed by [32], see Table 3, and applied to the relevant Generic SMR-300 layout drawings with example categorisation and classifications provided for those SSCs delivering the nuclear security functions of Delay, Detect, Assess, Access Control, Insider Threat Measures and Response. The framework used for the determination of Security Outcomes, Responses and Postures (SORPs) is prescribed by ONR via the Official Sensitive Annexes to SyAPs [15]. Plots of security zone locations derived in [32] are provided in Appendix D.

Table 3: Preliminary Security Zones

Security Zone	Description of Area	Notes
1	An area containing an HCVA	In line with [39] it was assumed that all Vital Areas are categorised as HCVA
2	An area which contains Category II NM or which is a VA and is outside Security Zone 1	All Vital Areas are assumed to be HCVAs ([39]) and within Security Zone 1. Material categorisation is obtained from [30].
3	An area which contains Group B ORM which is outside Security Zone 1 or 2	This area is defined in this assessment as an area containing NM/ORM other than fuel, which is outside Security Zones 1 and 2.
4	Baseline Area	This is an area containing other assets requiring protection as identified in subsection 7.5.3.1.

7.5.3.4 Security Infrastructure

An outline of the approach to develop the SI is shown in Figure 20 below.

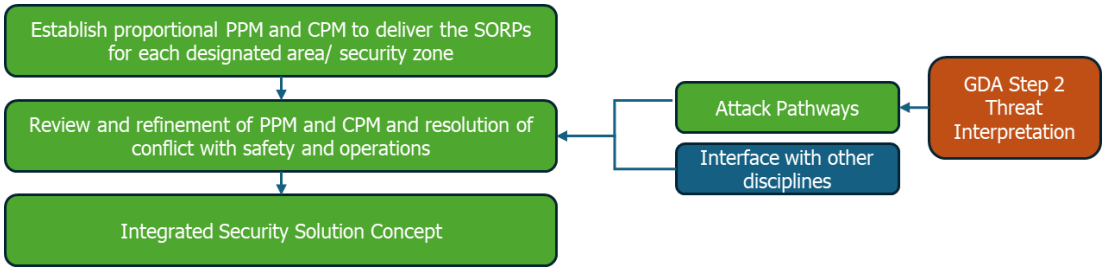

Figure 20: Outline Security Infrastructure Definition Approach

[32] presents a comprehensive list of physical protective measures (PPM), cyber protective measures (CPM) and insider protective measures which are mapped to the required security function(s) and which can be utilised to provide a multi-layered and graded security solution.

7.5.3.5 Development of an Integrated Security Solution

The SA identified the physical and cyber SORPs that need to be achieved in order to deliver appropriate levels of security, and the SI provided evidence that its outline solution of Protective Security Measures will meet these requirements (with the exception of a response force).

The CPS requires both physical and cyber measures to meet the CPS SORPs fully. The physical measures prevent an adversary from reaching the location, including the insider, and the cyber measures both prevent and mitigate the cyber-attack. The cyber measures are derived from Control Sets that are applied to the CBSIS.

All of these measures have been combined in [32] to show an indicative ISS. In addition, a concept of operations is outlined to indicate how it is operated to ensure the effective delivery of the required security outcomes and to identify any specific additional factors which need to be considered for a UK SMR-300. This is site-specific and licensee dependent and, so, it is outside the scope of GDA. However, for completeness, and to provide a link between the CSA and operations [32] presents a high-level description of an expected CONOP for a UK SMR-300.

7.6 Security Operations

The ISS will form the basis for the day-to-day protection of the SMR-300 site from sabotage and theft of NM/ORM or SNI. This protection will be site-specific and it will be the responsibility of the licensee and delivered via the licensee's site security operations, as required by [14].

The future licensee will develop a site security plan which will cover the nuclear site security operations alongside commercial and personnel security. This site security plan will be compatible with the plant's concept of operations and, in turn, form part of the overall site operational plan. A list of example topics which are expected to form part of the security plan is provided in the CSA Report [32].

While outside of the GDA scope of work, the human performance aspects identified within SyAPs, in particular in support of FSyP 1 (Leadership and Management for Security), FSyP 2 (Organisational Culture), FSyP 3 (Management of Human Performance), FSyP 8 (Workforce Trustworthiness) and FSyP 9 (Policing and Guarding) are recognised as being an important consideration of the development of arrangements for a future SMR-300 site in the UK. These aspects are captured as expectations on a future UK SMR-300 site licensee in Appendix D.

Nuclear security operations will start with the securing of the site prior to commencement of construction and will be expanded proportionately as the plant is commissioned and is fully in place and tested prior to the arrival of the first new fuel at the site. It thereafter continues until decommissioning and removal of nuclear material from the site with regular reviews and testing.

7.7 Application of the Secure by Design Principle

The Secure by Design Study [34], summarises how Holtec Britain and Holtec International have applied the SbD principle and methodology prior to, and during, GDA Step 2. This details how the generic SMR-300 design has been subject to security considerations from early concept design by the Holtec International SMR security team. This is considered to have provided a significant influence in the elimination and reduction of security vulnerabilities relating to the overall design of the plant.

During GDA Step 2, the UK security assessments of the SMR-300 were successful in identifying SbD design options to eliminate and reduce security-related issues and vulnerabilities which are being progressed via Holtec Britain's design challenge process.

[34] demonstrates how robust inherent security decision making has been used throughout the design of the generic SMR-300. The UK security team has also been proactively involved in providing security-related inputs into other GDA assessments and design challenges as required throughout GDA Step 2.

Holtec Britain is following the UK SMR-300 Design Management Process [46] to review and assess UK prospective design challenges and US-originated design changes to the GDA DRP. [34] demonstrates how SbD design challenges are considered in the prospective design change assessment process.

The identified SbD design options from the GDA Step 2 security assessments will be managed via the appropriate route as established by Holtec Britain to manage potential design challenges and changes. The appropriate recording and management of this process for SbD Options is identified as a GDA Security Undertaking, see subsection 7.8.

The timescales and design maturity of the Generic SMR-300 means that fully worked up design changes will not be developed and implemented for accepted changes until after GDA Step 2 is completed. Each potential design change arising from the GDA is logged into the UK Design Risk Register developed during Step 2 [46].

7.8 GDA Undertakings

Two principal GDA Security Undertakings have been identified during the GDA process for future enactment. Both have been formally captured by the appropriate mechanism [47] to ensure that they are carried into the site-specific phase of security planning. This is presented in Table 4 below.

Table 4: GDA Security Undertakings

GDA Security Undertaking	Capture Process
The UK DBT will inform future security assessments of the SMR-300.	Presented for inclusion in the Commitments, Assumptions & Requirements (CAR) Register.
SbD options will be carried forward into future design iterations and the site-specific planning stage.	Represented within the project risk register for inclusion in the future security planning cycle.

7.9 Expectations on a Future Licensee

In addition to the GDA Undertakings listed in Table 4, this GSR has identified a number of areas where expectations are placed on a future licensee to expand the scope of the security assessments, refine analyses or develop their own arrangements to comply with legal or regulatory requirements post-GDA. For completeness, these are listed in Table 5 below and are linked to the section of this GSR where the expectation is identified.

Table 5: Expectations on a Future UK SMR-300 Licensee

No.	Expectation	GSR Section
1	GDA Step 2 security assessments will be reviewed and updated during site-specific assessments to reflect changes in scope, design, information and threat as appropriate.	7.1
2	Post-GDA security assessments will consider further assets for protection beyond those addressed in GDA, including systems and equipment associated with emergency response, security and safeguards.	6.1
3	SNI located on the SMR-300 site will be assessed during future site-specific assessments.	6.1
4	The future licensee will develop a site security plan which will cover the nuclear site security operations alongside commercial and personnel security.	7.6

No.	Expectation	GSR Section
5	A future licensee will establish and maintain organisational security capability which meets the expectations of FSyP 1.	0
6	A future licensee will encourage and embed an organisational culture that recognises and promotes the importance of security to meet the expectations of FSyP 2.	0
7	A future licensee will implement and maintain effective arrangements to ensure the human contribution to delivery of security is understood and appropriately, implemented and resourced to meet the expectations of FSyP 2.	0
8	A future licensee will implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security to meet the expectations of FSyP 3.	0
9	A future licensee will implement and maintain effective supply chain management arrangements for the procurement of products or services related to nuclear security to meet the expectations of FSyP 4.	0
10	A future licensee will design and support their nuclear security regime to ensure it is reliable, resilient and sustained throughout the entire lifecycle to meet the expectations of FSyP 5.	0
11	A future licensee will implement and maintain a proportional physical protection system that integrates technical and procedural controls to form layers of security that build defence-in-depth and are graded according to the potential consequence of a successful attack to meet the expectations of FSyP 6.	0
12	A future licensee will have in place appropriate Cyber Security and Information Assurance (CS&IA) arrangements to comply with FSyP 7 and all the associated SyDPs.	0
13	A future licensee will have in place an effective workforce trustworthiness review in compliance with FSyP 8 and all the associated SyDPs.	0
14	A future licensee will demonstrate effective guarding and policing arrangements, integrating the operations of relevant police forces and security guard services to meet the expectations of FSyP 9.	0
15	A future licensee will implement and maintain effective security emergency preparedness and response arrangements which are integrated with the wider safety arrangements to meet the expectations of FSyP 10.	0

8.0 REFERENCES

[1] Holtec Britain, "HI-2240261 Preliminary Security Report," Revision 1, February 2024.

[2] Holtec Britain, "HI-2240648, GDA Design Reference Point," Revision 2, March 2025.

[3] Holtec Britain, "HI-2240121, SMR-300 UK Generic Design Assessment Scope," Revision 1, June 2024.

[4] Holtec Britain, "HI-2240260, Preliminary Safeguards Report," Revision 2, May 2025.

[5] Holtec Britain, "HPP-3295-0019, Classification Policy and Guidance Document," Revision 0, 2024.

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

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

[8] United Nations, "International Convention for the Suppression of Acts of Nuclear Terrorism," April 2005.

[9] International Atomic Energy Agency, "Nuclear Security Series No. 20, Nuclear Security Fundamentals, Objective and Essential Elements of a State's Nuclear Security Regime," 2013.

[10] International Atomic Energy Agency, "INFCIRC/225/Revision 5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," 2011.

[11] International Atomic Energy Agency, "48-T, Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities," 2024.

[12] International Atomic Energy Agency, "NSS No 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities," 2018.

[13] Western European Nuclear Regulators Association, "Interfaces between Nuclear Safety and Nuclear Security," April 2019.

[14] HM Government, "Nuclear Industries Security Regulations (NISR) 2003," Statutory Instrument 2003 No. 403.

[15] Office for Nuclear Regulation, "Security Assessment Principles 2022 Edition," Version 1, 2022.

[16] Office for Nuclear Regulation, "CNS-TAST-GD-6.1, Categorisation for Theft," Issue 2.1, April 2025.

[17] Office for Nuclear Regulation, "CNS-TAST-GD-6.2, Categorisation for Sabotage," Issue 2, March 2023.

[18] Office for Nuclear Regulation, "CNS-TAST-GD-6.3, Physical Protection System Design," Issue 2, April 2022.

[19] Office for Nuclear Regulation, "CNS-TAST-GD-7.3, Protection of Nuclear Technology and Operations," Revision 0, March 2017.

[20] Office for Nuclear Regulation, "CNS-TAST-GD-11.4.1, Secure by Design," Issue 1.1, January 2023.

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

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

[23] Office for Nuclear Regulation, "CNS-TAST-GD-7.1, Effective Cyber and Information Risk Management," Issue 2.1, September 2024.

[24] Office for Nuclear Regulation, "CNS-TAST-GD-7.5, Protection and Response to Cyber Security Incidents," January 2024, Issue 4.

[25] Office for Nuclear Regulation, "CNS-TAST-GD-11.1, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs," Issue 1.2, May 2021.

[26] Office for Nuclear Regulation, "ONR-GDA-GD-006, Guidance to Requesting Parties on the Generic Design Assessment (GDA) process for safety and security assessments of new Nuclear Power Plants (NPP)," Issue 1, August 2024.

[27] Office for Nuclear Regulation, "ONR-GDA-GD-007, New Nuclear Power Plants: Generic Design Assessment Technical Guidance," Revision 0, May 2019.

[28] Holtec Britain, "HI-2240873, SMR-300 Secure by Design Methodology," Revision 0, August 2024.

[29] Holtec Britain, "HI-2240874, SMR-300 Cyber Security Risk Assessment Methodology," Revision 0, September 2024.

[30] Holtec Britain, "HI-2240871, SMR-300 Theft Methodology & Analysis," Revision 0, August 2024.

[31] Holtec Britain, "HI-2240880, SMR-300 Vital Area Identification & Categorisation Methodology," Revision 0, August 2024.

[32] Holtec Britain, "HI-2240877, Conceptual Security Arrangements," Revision 0, March 2025.

[33] Holtec International, "HI-2240077, SMR-300 Plant Overview," Revision 1, April 2024.

[34] Holtec Britain, "HI-2240879, Secure by Design Study," Revision 0, March 2025.

[35] Holtec Britain, "HI-2241013, Holtec SMR-300 GDA CAE Model Report," Revision 2, 2025.

[36] Holtec Britain, "HI-224006, SMR-300 GDA Safety, Security and Environmental Case Structure," Report No.4, January 2024.

[37] Holtec International, "HPP-160-3012, SMR-160 Design Standards for Security and Safeguards," Revision 0, August 2018.

[38] Mott MacDonald, "100110593-ENG1-0036, HI-2240120, Holtec SMR GDA Fundamental Design Philosophy Report," Revision A, February 2024.

[39] Holtec Britain, "HI-2240875, SMR-300 Vital Area Identification and Categorisation Study," Revision 0, February 2025.

[40] HM Government, "Department for Energy Security and Net Zero, UK Design Basis Threat".

[41] Holtec Britain, "HI-2240872, SMR-300 Threat Interpretation for GDA Step 2," Revision 0, August 2024.

[42] International Atomic Energy Agency, "IAEA Nuclear Security Series No. 10-G, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements," Revision 1, 2021.

[43] Holtec Britain, "HI-2240876, Cyber Security Risk Assessment Study," Revision 0, February 2025.

[44] International Electrotechnical Commission, "Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements," IEC 62645:2019, November 2019.

[45] International Electrotechnical Commission, "IEC 63096, Niclear Power Plants - Instrumentation, Control and Electrical Power Systems - Security Controls," 2020.

[46] Holtec Britain, "HPP-3295-0017, Design Management," Revision 1, December 2024.

[47] Holtec Britain, "HPP-3295-0013, Holtec SMR-300 Generic Design Assessment Capturing and Managing Commitments, Assumptions and Requirements," Revision 1, January 2025.

[48] Office for Nuclear Regulation, "CNS-TAST-GD-7.2, Information Security," August 2023.

[49] Office for Nuclear Regulation, "CNSS-SEC-GD-002, Nuclear Industry Security Regulations 2003-Guidance for Inspectors," Issue 1, Mar 2022.

[50] Office for Nuclear Regulation, "Report: 2023/25878, Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Inherent Risk Profile Questionnaire".

[51] HM Government Cabinet Office, "Security Policy Framework," December 2022.

[52] Office for Nuclear Regulation, "Report: 2023/25877, Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Evidencing Expectations, System Question Set," April 2023.

[53] Office for Nuclear Regulation, "Report: 2023/25876, Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Evidencing Expectations, Facility Question Set," April 2023.

[54] Office for Nuclear Regulation, "Report: 2023/25874, Nuclear Industry Security Regulations, Regulation 22 Dutyholder – Evidencing Expectations, Corporate Question Set," April 2023.

[55] Office for Nuclear Regulation, "Security Classification Policy".

[56] Holtec Britain, "CD-44, Security Manual".

[57] Holtec Britain, "HPP-3295-0027, Security Organisation".

[58] Holtec Britain, "HPP-3295-0023, Security Risk Assessment, Risk Register and Risk Treatment Plan".

[59] Holtec Britain, "HPP-3295-0011, Handling and Protecting Security Marked Documentation".

[60] Holtec Britain, "HPP-3295-0020, Security Breaches and Incident Management".

[61] Holtec Britain, "HPP-3295-0024, Supply Chain and Contracting Management".

[62] Holtec Britain, HPP-3295-0026, (Security) Management Review Policy and Process.

[63] Holtec Britain, "CD 23, Disaster Coping and Recovery Plan".

[64] Holtec Britain, "CD 26, IT Disaster Recovery Plan".

[65] Holtec Britain, "HPP-3295-0025, Holtec Britain Manage Visitors".

[66] Risktec Solutions Limited, "HLTB-01-R-05, Physical Security Assessment".

[67] Risktec Solutions Limited, "HLTB-01-R-23, Review of List N security arrangements in support of self-certification," Issue 1.0, November 2024.

[68] Holtec Britain, "HPP-329-0005, GDA Competency and Training Procedure".

[69] Holtec Britain, "HPP-3295-0022, Personnel Security Company Practice".

[70] Holtec Britain, "HPP-3295-0021, Personnel Security Aftercare Company Practice".

[71] HM Government, "Report No. GovS 007: Security, Government Functional Standard," Version 2.0, 2021.

9.0 LIST OF APPENDICES

Appendix A Compliance with the Nuclear Industries Security Regulations A-1

Appendix B Security Claims, Arguments and Evidence..... B-1

Appendix C Generic SMR-300 Candidate Vital Area Locations..... C-1

Appendix D Generic SMR-300 Illustrative Security Zones..... D-1

Appendix E Compliance with Fundamental Security and Security Delivery Principles..... E-1

Appendix F Demonstration of the Security ‘Golden Thread’ F-1

Appendix A Compliance with the Nuclear Industries Security Regulations

A.1 Introduction

NISR 2003 [14] places legal requirements on organisations to protect NM and ORM from sabotage and theft as well as to protect SNI from theft, loss or unauthorised disclosure. This means that:

(a) Holtec Britain and their supply chain have the legal requirement (under Part 4, Regulation 22 of NISR 2003) to protect against loss, theft or unauthorised disclosure of, or unauthorised access to SNI whenever it is stored, processed, transmitted or accessed during the SMR-300 GDA and design development.
(b) A future UK SMR-300 licensee will have a legal requirement (under Part 2, Regulations 4 to 12 of NISR 2003) to implement an approved security plan to protect NM and ORM at the site from sabotage and theft and to protect against the compromise or loss of SNI within the site.
(c) A future UK SMR-300 licensee will have a legal requirement (under Part 4, Regulations 22 of NISR 2003) to implement an approved security plan to protect against the compromise or loss of SNI where it is held at locations which belong to the licensee but are not within the licensed site, or which belong to the suppliers within nuclear supply chain used by the licensee for processing and storing SNI on their behalf.

The following sections provide a description of the processes that Holtec Britain has developed and adopted to:

- Comply with the requirements of Regulation 22 of NISR 2003 during the GDA and design development stage; and
- Facilitate compliance by a future UK SMR-300 licensee with the requirements of Regulations 4 to 12 and 22 of NISR thereafter.

A.2 SMR-300 GDA and Design Development

This section describes how Holtec Britain has complied with the requirements of NISR 2003 [14] during the SMR-300 GDA and will comply during design development post-GDA.

A.2.1 SMR-300 GDA Protection of SNI

Holtec Britain developed a pathway to deliver its legal requirement under Regulation 22 of NISR 2003 to protect SNI. The pathway was informed by the ONR SyAPs [15] and supporting ONR guidance [48] [49] and delivered the security management arrangements which follow a graded approach which is proportional to risk based on the quantity and type (hard copy and/or digital) of SNI held.

The risk was established using the Inherent Risk Profile (IRP) Questionnaire [50], developed by ONR. The pathway recognised that the IRP level would change for Holtec Britain as the project developed through GDA and beyond to site licensing and operations. A high-level illustration of the pathway showing the change in IRP level and graded security arrangements is presented in Figure 21.

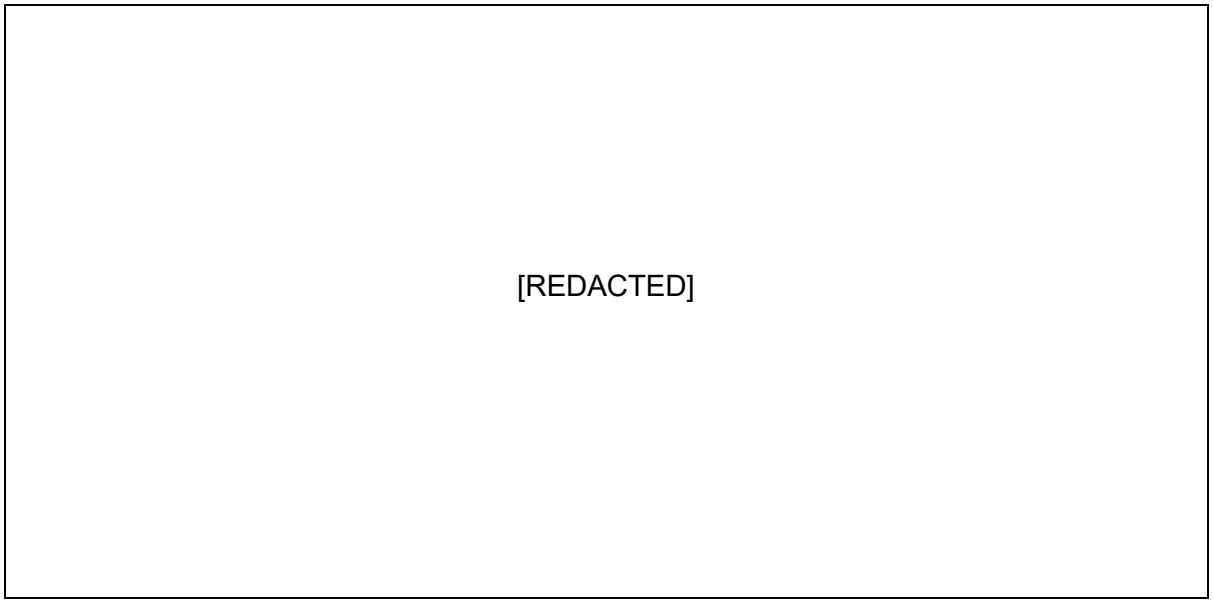

Figure 21: List N Pathway

The key steps comprising the pathway are described below.

A.2.2 Preparation Phase - Pre-GDA

In preparation to enter the GDA, Holtec Britain undertook a review of its existing security management system relative to His Majesty's Government (HMG) Security Policy Framework (SPF)[7] [51]. The review made use of the ONR Evidencing Expectations [52] [53] [54] to identify gaps relative to the five applicable FSyPs[8] for the different IRP levels:

- FSyP 1 – Leadership and Management for Security.
- FSyP 2 – Security Organisational Culture.
- FSyP 3 – Management of Human Performance.
- FSyP 7 – Cyber security and Information Assurance.
- FSyP 8 – Workforce Trustworthiness.

The review covered the five key elements comprising a security management system, as illustrated in Figure 22[9] .

[7] The HM Government Functional Standard GovS 007 [71] has replaced the Security Policy Framework. However, the policies which sit within the SPF remain in effect but are now in support of GovS 007.
[8] ONR considers that these five FSyAPs provide a framework for compliance with [71].
[9] The physical security review included a review of the security arrangements at the designated List N facility.

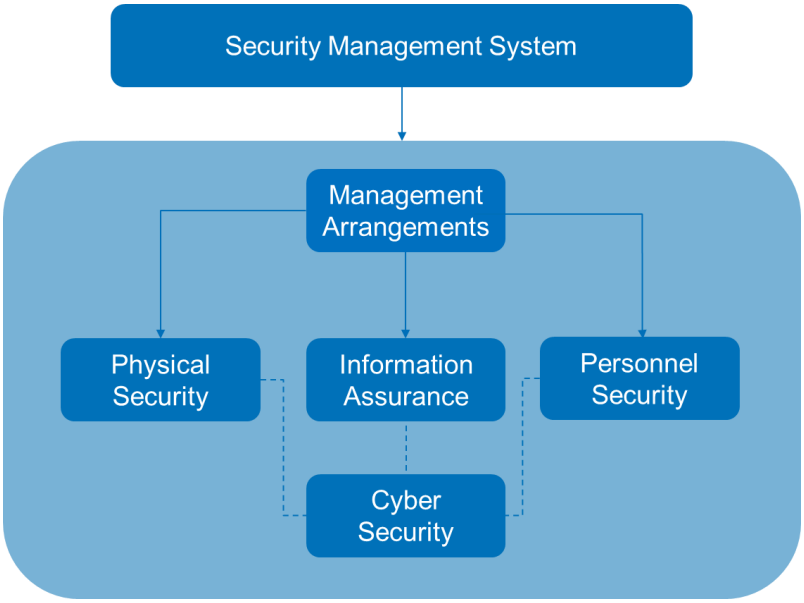

Figure 22: Key Elements of a Security Management System

The outcomes of the review were consolidated and subsequently used to develop a list of activities required to implement the required security management arrangements covering the following areas at the different IRP levels:

Table 6: Pathway Activities

Pathway Activities
Security Policy
Security Organisation
Threat Policy
Security Risk Appetite for SNI
Security Risk Assessment, Risk Register and Risk Treatment Plan
Classification Policy
Handling and Protecting of for Classified Assets
Security Breaches and Incident Management
Supply Chain and Contracting Management
Management Review Policy and Process
Business Continuity and Disaster Recovery Policy
Facility Risk Assessment
Company Security Instructions
Competence and Training Management
Personnel Security Vetting and Aftercare Requirements Process
Information Technology Security

A.2.3 GDA Step 1

The IRP level during the SMR-300 GDA Step 1 was assessed as 'Very Low' as no hardcopy or digital SNI was expected to be held during this step. The existing Holtec Britain corporate information security management arrangements (referred to as 'foundation security arrangements' in Figure 21) were assessed to be suitable for this Step.

A.2.4 GDA Step 2

Holtec Britain became a Contracting Authority as part of the preparation for entering GDA Step 2. [REDACTED].

To this end, the activities listed in Table 6 were progressed during GDA Step 1 so that appropriate security arrangements were in place at the Bristol Office to produce, store, handle and/or destroy physical O-S:SNI at the start of GDA Step 2. The security arrangements developed and implemented are presented in Table 7 which provides an overview of the security arrangements which have been developed and implemented against the actions identified in the pathway. In addition it provides a link from the arrangements to the applicable FSyPs to demonstrate compliance against NISR Regulation 22.

The assessed IRP level increased to 'Low' during the SMR-300 GDA Step 2. This is because of an increasing requirement to produce and process hard copy and digital SNI during this step. This SNI was classified at O-S:SNI only [55]. This was principally achieved by using suitable threat information derived from publicly available information see subsection 7.4. The assessed IRP risk remained at Low throughout the GDA as the number of documents in either digital or hardcopy did not meet the criteria for a Medium IRP.

[REDACTED]

Table 7: Security Arrangements and Compliance against SyAPs

Pathway Activities	Security Management Arrangements	Applicable FSyP
Security Policy	CD 44- Holtec Britain Security Manual [56]	FSyP 1, 2 and 7
Security Organisation	HPP-3295-0027- Holtec Britain Security Organisation [57]	FSyP 1, 3, 7 and 8
Threat Policy	CD 44- Holtec Britain Security Manual [56]	FSyP 1, 2, 7 and 8
Security Risk Appetite for SNI	CD 44- Holtec Britain Security Manual [56]	FSyP 1, 7 and 8
Security Risk Assessment, Risk Register and Risk Treatment Plan	HPP-3295-0023- Holtec Britain Security Risk Assessment, Risk Register and Risk Treatment Plan. [58]	FSyP 1, 7 and 8
Classification Policy	HPP-3295-0019 Classification Policy and Guidance [5]	FSyP 3, 7 and 8
Handling and Protecting of for Classified Assets	HPP-3295-0011 –Handling and Protecting Security Marked Documentation [59]	FSyP 3, 7 and 8
Security Breaches and Incident Management	HPP-3295-0020 – Security breaches and incident management [60]	FSyP 1, 7 and 8
Supply Chain and Contracting Management	HPP-3295-0024 Supply Chain and Contracting Management [61]	FSyP 2, 7 and 8
Management Review Policy and Process	HPP-3295-0026 – Management Review Policy and Process [62]	FSyP 1, 2, 7 and 8

Pathway Activities	Security Management Arrangements	Applicable FSyP
Business Continuity and Disaster Recovery Policy	CD 23 - Disaster Coping and Recovery Plan [63] CD 26 - IT Disaster Recovery Plan [64]	FSyP 1 and 7
Visitor Management	HPP-3295-0025 – Holtec Britain Manage Visitors [65]	FSyP 1, 7 and 8
Facility Risk Assessment	HLTB-01-R-05 – Physical Security Assessment [66] HLTB-01-R-23 _Review of Security Arrangements [67]	FSyP 7
Company Security Instructions	CD 44- Holtec Britain Security Manual [56]	FSyP 1, 2, 3, 7 and 8 (Note these company instructions provides supporting instructions to all procedures)
Competence and Training Management	HPP-329-0005- GDA Competency and Training Procedure [68]	FSyP 1, 2, 3, 7 and 8
Personnel Security Vetting and Aftercare Requirements Process	HPP-3295-0022 – Personnel Security Company Practice [69] HPP-3295-0021- Personnel Security – Aftercare Company Practice [70]	FSyP 2, 3, 7 and 8
Information Technology Security	Post GDA Step 2	FSyP 7

[REDACTED]

A.3 Design Development Post-GDA

The IRP level is expected to increase during the design development post-GDA. This is because the site-specific SMR-300 detailed design (including the design of the security systems) and site licensing activities will require an increasing amount of SMR-300 O-S:SNI to be held at several Holtec Britain and (potentially) Holtec International offices as well as at an increasing number of supply chain vendor locations. Additionally, there will be a need to produce, process and store SECRET (S) level information.

A.3.1 Role transition of Contracting Authority and Future UK SMR-300 Licensee Post GDA

The Duty Holder role of Holtec Britain will transition from Contracting Authority to List N Duty Holder during the Design Development post-GDA. Initially, Holtec Britain will remain as the Contracting Authority, where it will be responsible under Regulation 22 for the approval of all systems and facilities and their locations, where SMR-300 SNI owned by Holtec Britain is stored and processed. However, once a UK SMR-300 licensee is identified, Holtec Britain will become a “Contractor” to that licensee and a List N Duty Holder organisation and the role of Contracting Authority will be assumed by the UK SMR-300 licensee, where they will be responsible under Regulation 22 for the approval of all systems and facilities and their locations of their nuclear supply chain.

A.3.2 Preparations for Handling SMR-300 SNI Post-GDA

To prepare for the expected increase in SMR-300 SNI post-GDA, it is anticipated that:

- A Holtec Britain UK owned and administered O-S:SNI classified network capable of satisfying the demands of post GDA security requirements will be developed and implemented, potentially across several offices. This will require the revision of the risk

assessment and the approval by the Holtec SIRO in accordance with security processes and approved by the Contracting Authority which may be Holtec Britain or Future UK SMR-300 Licensee (see A.3.1).

- Other locations and the systems and facilities within them (Holtec Britain, Holtec International and supply chain vendor offices) will be inspected and approved by the Holtec Britain SIRO and/or by the Contracting Authority (see A.3.1) to hold SMR-300 O-S:SNI and/or S commensurate with the IRP level for the physical (hard copy) and electronic (digital) systems at the location(s) and declared on List N. For O-S:SNI this may include Holtec International offices in the US.

To prepare for the handling of S level information, it is anticipated that:

- A standalone classified network (system) with supporting infrastructure will be established at a Holtec Britain List N location in the UK and the security management arrangements and protective controls at that location enhanced accordingly. The S level arrangements will require a risk assessment and the approval by the Holtec SIRO in accordance with security processes and approval by the Contracting Authority (see A.3.1) prior to its use and declaration on List N as a system approved to hold SMR-300 related S level information.
- There will be a small number of supply chain locations that will require to handle SMR-300 information classified as S. These systems, facilities and their locations will require assessment and approval by the Contracting Authority under NISR 2003 Regulation 22 and added to List N.

A.4 Protection of Nuclear Material and SNI

Responsibility for compliance with NISR 2003 at an SMR-300 site lies with the site licensee. The site licensee will develop and implement a site security plan approved by ONR to protect against the sabotage or theft of nuclear material and against the compromise or loss of SNI within the site in compliance with Parts 2 and 4 of NISR 2003.

The development of the site security plan will be informed by this GSR, and design activities carried out by Holtec Britain and its parent company Holtec International. This includes SbD activities and the development and illustrative implementation of security assessment methodologies (e.g., VAI&C, theft and CSRA methodologies) carried out during Steps 1 and 2 of the GDA.

These activities are being carried out by Holtec Britain in accordance with the ONR SyAPs (including Appendices A to E and H to J) and informed, by the principles listed below. This will enable Holtec Britain to deliver a site-specific SMR-300 design that will support the SMR-300 licensee's compliance with NISR 2003.

- Key Security Plan Principles (KSyPP)
    - KSyPP 1 – Secure by Design.
    - KSyPP 2 – The Threat.
    - KSyPP 3 – The Graded Approach.
    - KSyPP 4 – Defence in Depth.

- Fundamental Security Principle (FSyP) and Security Delivery Principles (SyDP)
    - FSyP 6 – Physical Protection System.
    - SyDP 6.1 – Categorisation for Theft.
    - SyDP 6.2 – Categorisation for Sabotage.
    - SyDP 6.3 – Physical Protection System Design.
    - FSyP 7 – Cyber Security and Information Assurance.
    - SyDP 7.1 – Effective Cyber and Information Risk Management.
    - SyDP 7.3 – Protection of Nuclear Technology and Operations.

Appendix B Security Claims, Arguments and Evidence

The CAE Model Report [35] presents the overall CAE model for the Generic SMR-300 SSEC. This includes the claims applied in this GSR which are presented within this Appendix.

Figure 23 presents the GSR Fundamental Objective (see also Section 6.0) and shows how it is broken down into seven SyCs. In turn, the SyCs are broken down into more refined sub-claims as necessary for the GDA Step 2 assessment. In some cases, for example the protection of SNI, the claim has not been broken down further due to the scope of the assessment at this stage.

As identified subsection 1.4, the GSR is a 'claims-level' document and hence Table 8 below maps the high level security claims to the sections of this GSR where they are discussed. Below the high level claims are a series of lower level claims (analogous to arguments and evidence) which are addressed primarily in the documentation supporting this GSR (as defined in Table 1).

Hence, Table 9 presents a route map of where each security sub-claim is addressed within the security documentation structure within the GDA Step 2 submission.

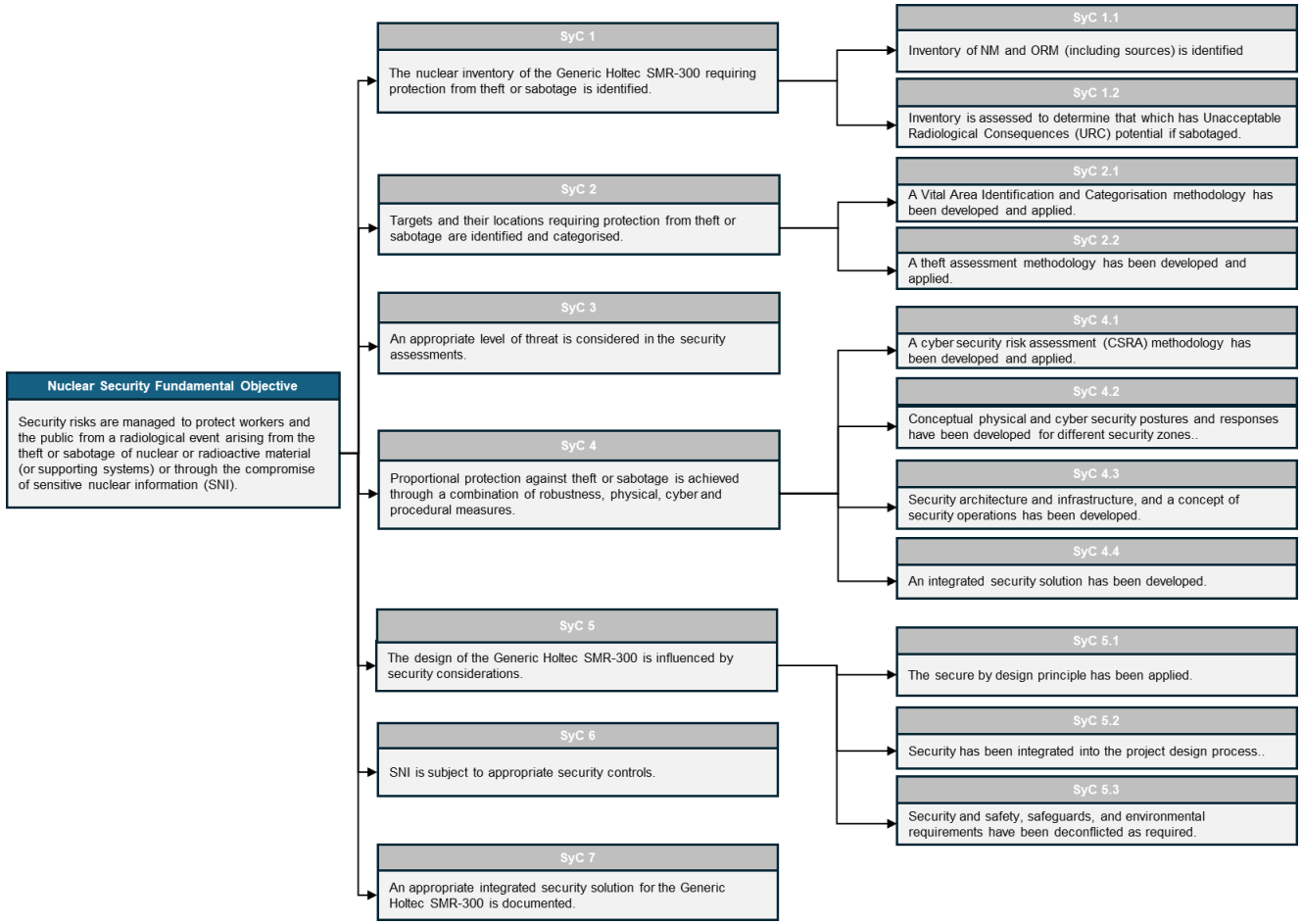

Figure 23: Security Claims and Sub-Claims

Table 8: Security Claims Map to GSR Section

SyC	Description	GSR Section(s)	Notes
1	The nuclear inventory of the Generic Holtec SMR-300 requiring protection from theft or sabotage is identified.	7.2	-
2	Targets and their locations requiring protection from theft or sabotage are identified and categorised.	7.3	-
3	An appropriate level of threat is considered in the security assessments.	7.4	Evolution of the threat to be applied in security assessments is outlined in Figure 13.
4	Proportional protection against theft or sabotage is achieved through a combination of robustness, physical, cyber and procedural measures.	7.5	-
5	The design of the Generic Holtec SMR-300 is influenced by security considerations.	7.7	-
6	Sensitive Nuclear Information is subject to appropriate security controls.	-	Out of scope for SMR-300 generic site. Appendix A outlines how SNI is managed by the project during GDA.
7	An appropriate integrated security solution for the Generic Holtec SMR-300 is documented.	7.5	-

Table 9: Security Sub-Claim map to GSR Supporting Document

Sub-SyC	Description	Supporting Document(s)	Status
1.1	[REDACTED]		
1.2	[REDACTED]		
2.1	[REDACTED]		

Sub-SyC	Description	Supporting Document(s)	Status
2.2	[REDACTED]		
4.1	A cyber security risk assessment methodology has been developed and applied.	CSRA Methodology [29] CSRA Study [43]	A full scope, flexible and extendable CSRA methodology is presented in [29]. [43] presents a demonstration of the implementation of this methodology which focuses on the PSS for GDA Step 2.
4.2	Conceptual physical and cyber security posture and response have been developed for different security zones.	Conceptual Security Arrangements [32]	[32] presents and provides an illustrative implementation of a framework which demonstrates the golden thread from the security risk assessments through to the development of suitable protective measures.
4.3	Security architecture and infrastructure, and a concept of security operations has been developed.	Conceptual Security Arrangements [32]	[32] presents and provides an illustrative implementation of a framework for SA, SI and CONOPs based on the limited-scope outputs of GDA Step 2 security risk assessment studies.
4.4	An integrated security solution has been developed.	Conceptual Security Arrangements [32]	[32] demonstrates the development of an illustrative ISS based on the limited-scope outputs of GDA Step 2 security risk assessment studies.
5.1	The secure by design principle has been applied.	Secure by Design Methodology [28] Secure by Design Study [34]	A full scope, flexible and extendable SbD methodology is presented in [28]. [34] presents a evidence of how SbD has been applied during the project to date, including in the development of the design to the declared DRP [2] and throughout the GDA.
5.2	Security has been integrated into the project design process.	Secure by Design Methodology [28] Secure by Design Study [34]	[28] presents details of how security is integrated into the design process, modification and optimisation process. [34] provides evidence that this integration has occurred up to the end of GDA Step 2.
5.3	Security and safety, safeguards, and environmental requirements have been deconflicted as required.	Secure by Design Methodology [28] Secure by Design Study [34]	[28] presents details of how deconfliction is considered within the SbD process. In GDA Step 2 this is mostly evidenced in [34] by the security team having a stakeholder role in the design challenge process. Wider scope deconfliction of the design, processes etc. will occur post GDA Step 2.

Appendix C Generic SMR-300 Candidate Vital Area Locations

[REDACTED]

Appendix D Generic SMR-300 Illustrative Security Zones

[REDACTED]

Appendix E Compliance with Fundamental Security and Security Delivery Principles

[REDACTED]

Appendix F Demonstration of the Security 'Golden Thread'

F.1 Introduction

[25] discusses the concept of the security 'golden thread' in broad terms as proving *a "thread that 'tells the story' from applying SyAPs principles through to the description of a conceptual design for security…to enable the potential licensee to develop the GSR document into a security plan thereby meeting relevant legal requirements"*.

In this sense, this GSR (and the supporting Tier 2 documents), developed to meet the GSR objectives outlined in subsection 1.2, provides this overall golden thread by identifying legislative requirements, RGP and SyAPs principles and demonstrating how these have been used to develop and apply appropriate assessment methodologies leading to the development of illustrative conceptual security arrangements during GDA Step 2.

To supplement this broad definition, this Appendix provides an illustration of the 'golden thread' of information which runs through the GDA Step 2 security assessments.

F.2 Golden Thread

In this Appendix, the term 'Golden Thread' is used to refer to the flow of information and results between the various assessments undertaken for the security risk assessment which ensures that each stage of assessment flows logically from one stage to another.

The Golden Thread ensures that a clear path can be followed throughout the assessment from the initial stage, which is the identification of the inventory of NM/ORM (see also subsection 7.2), through the sabotage and theft assessments (40] and [30] respectively and summarised in subsections 7.3.2 and 7.3.3) to the illustrative Security Zones defined and categorised in [32] which are summarised in subsection 7.5.3.3 and presented in full in Appendix D, and their required SORPs.

This Golden Thread is illustrated in Figure 24 and is illustrated further in this Appendix through use of examples.

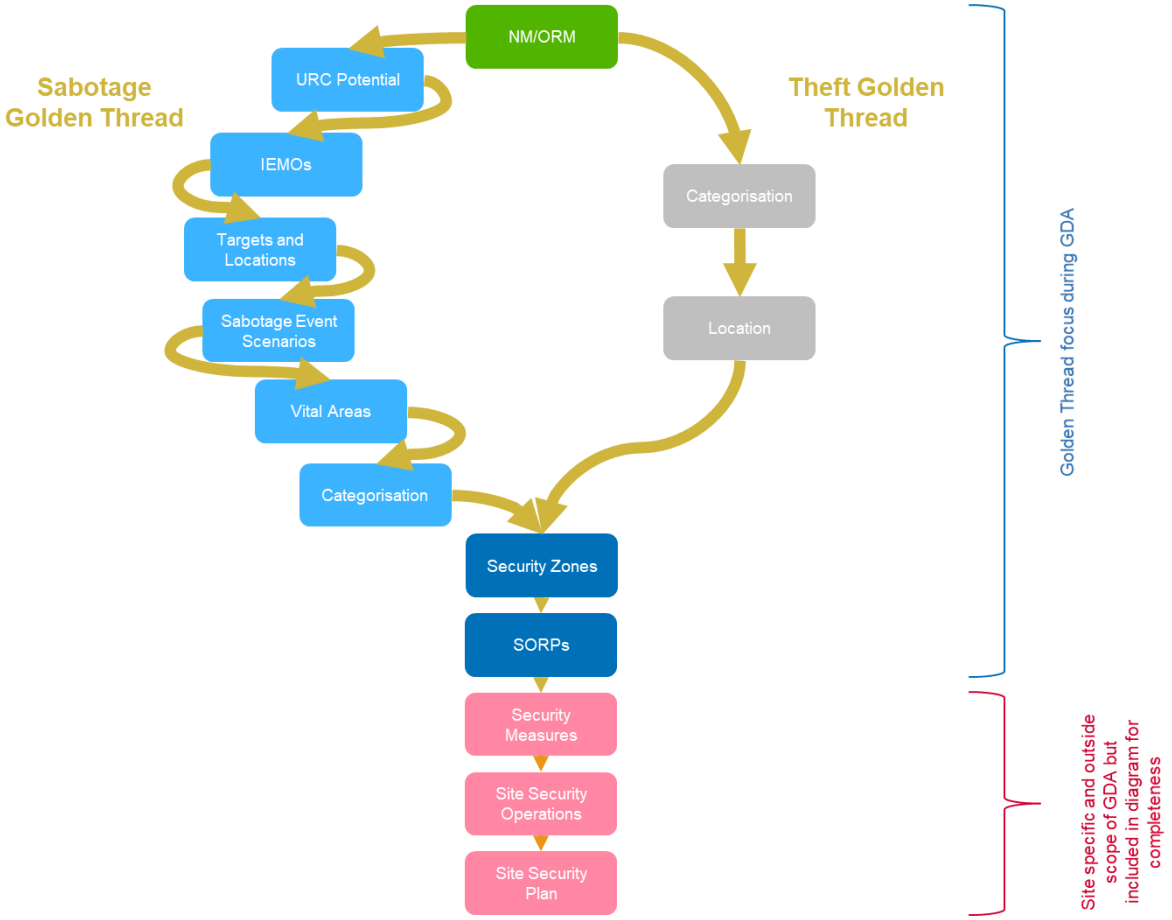

Figure 24: Golden Thread

F.3 Sabotage

In the case of sabotage assessment, the 'Golden Thread' represents the clear and auditable linking of NM/ORM with URC potential, through the identification of IEMOs and sequences of sabotage actions (SES), and their locations, to the identification of areas requiring protection (Vital Areas) through to the designation of security zones and the security outcomes, responses and postures which must be achieved. This enables a logical and coherent security case to be developed which provides a robust demonstration of the outcomes to be achieved by the security design.

NM/ORM

Therefore, for sabotage the GDA assessment begins at the inventory of NM/ORM presented within the VAI&C Study [39] for material located within CS. This study highlights that **used/spent fuel** is located in the CS.

[REDACTED]