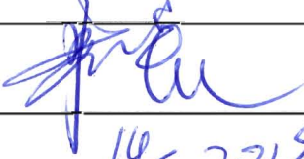




Revision	Approved by	Number of Pages
000		46
Approval Date		
 <p>General Nuclear System Ltd.</p>		
<p>UK HPR1000 GDA Project</p>		
Document Reference:	HPR/GDA/GSR/0001	
<p>Title:</p> <p style="text-align: center;">Generic Security Report</p>		
<p>This document has been prepared on behalf of General Nuclear System Limited (GNS) with the support of China General Nuclear Power Corporation (CGN) and Électricité de France S.A. (EDF).</p> <p>Although due care has been taken in compiling the content of this document, neither GNS, CGN, EDF nor any of their respective affiliates accept any liability in respect to any errors, omissions or inaccuracies contained or referred to in it.</p>		

DISTRIBUTION LIST

Recipients	Cross Box
GNS Executive	<input checked="" type="checkbox"/>
GNS all staff	<input type="checkbox"/>
GNS and BRB all staff	<input type="checkbox"/>
CGN	<input type="checkbox"/>
EDF	<input type="checkbox"/>
Regulators	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 4/46

TABLE OF CONTENTS

1. List of Abbreviations and Acronyms	7
2. Executive Summary.....	10
3. Public Release of Generic Security Report	12
4. Introduction.....	13
5. Generic Security Report (GSR) Route Map	14
6. General Nuclear System (GNS) Approach to GDA	15
6.1 General	15
6.2 GDA Scope	16
6.3 GNS The Organisations	16
6.4 Lead Project Correspondents	17
6.5 Third Party Service Provision.....	17
6.6 Governance.....	18
7. General Nuclear System (GNS) – The GDA Process	18
8. General Nuclear System (GNS) Approach to GSR.....	20
9. GNS Approach to Regulation and Reference Material	22
9.1 Security Assessment Principals (SyAPs).....	23
9.2 ONR CNS Assessment Plans.....	24
9.3 ONR Technical Meetings	24
9.4 Regulatory Queries (RQs), Regulatory Observations (ROs), Regulatory Issues (RIs).....	24
9.5 Relevant Good Practice	24
9.6 Suitably Qualified Experienced Persons	25
10. Terminology	25
11. Interactions with Others.....	25
11.1 UK HPR 1000 CGN/GNS SMEs	25

11.1.1	Security Informed Design	25
11.1.2	Optimum Design for the UK HPR1000	26
11.1.3	Consistency with PCSR and PCER.....	26
11.2	CGN Physical Protection Group	27
11.3	Regulators	28
11.3.1	ONR.....	28
11.3.2	EA.....	28
11.4	BRB	28
11.5	Public	28
12	UK HPR Plant Information	28
12.1	Introduction to UK HPR1000	28
12.2	Use of Plant Information.....	30
13	GNS Security Risk Management Approach.....	31
13.1	Introduction to Security Risk Management Approach.....	31
13.2	Security Regime Model.....	32
13.3	Benefits of Approach	32
14	Vital Area Identification Methodology.....	33
14.1	VAI Methodology Overview	34
14.2	Cyber Risk Assessment Methodology	34
14.2.1	Methodology Overview	35
15	GSR Security Case	35
15.1	General.....	35
15.2	SSER & GSR.....	36
15.3	GSR Approach to Claims, Arguments and Evidence	37
16	Security Regime Operation CONOP.....	39
16.1	Security Regime Operation CONOP	39
16.2	Detail of Security Regime Operation	39
17	Evolution of GSR V0 - V2	41

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 6/46

18. References 41

Appendix 10A Terminology and Definitions 43

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 7/46

1. List of Abbreviations and Acronyms

ALARP	As Low As Reasonably Practicable
BPC&I	Basic Process Control & Instrumentation Systems
CBSIS	Computer Based Systems Important to Safety
CBSY	Computer Based Security Systems
CGN	China General Nuclear
CNI	Civil Nuclear Industry
CONOP	Concept of Operation
CPS	Cyber Protection System
CS&IA	Cyber Security & Information Assurance
DBT	Design Basis Threat
EA	Environment Agency
EDF	EDF Energy
FCG3	Fangchenggang Nuclear Power Plant Unit 3
FSyP	Fundamental Security Principle
GDA	Generic Design Assessment
GNS	General Nuclear Systems Limited
GSR	Generic Security Report
GSyC	Generic Security Claim
HCVA	High Consequence Vital Area
HPR1000	Hua-long Pressurised Reactor
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IEC	International Electro-technical Commission
IEMO	Initiating Events of Malicious Origin
IT	Information Technology
N/A	Not Applicable
NI	Nuclear Island

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 8/46

NIMCA	Nuclear Industries Malicious Capabilities (Planning) Assumptions
NISR	Nuclear Industries Security Regulations 2003
NIST	National Institute of Standards and Technology
NM	Nuclear Material
NMAC	Nuclear Material Accountancy & Control
NORMS	National Objectives, Requirements & Model Standards
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ONR(CNS)	ONR Civil Nuclear Security
OPEX	Operational Experience
ORM	Other Radioactive Material
ORPP	Operational Research, Planning & Preparation
OT	Operational Technology
PCEC	Programmable Complex Electronic Components
PCER	Pre-Construction Environmental Report
PCSR	Pre-Construction Safety Report
PPS	Physical Protection System
PWR	Pressurised Water Reactor
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
SAA	Severe Accident Analysis
SBI	Sensitive Business Information
SME	Subject Matter Expert
SNI	Sensitive Nuclear Information

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 9/46

SoDA	Statement of Design Acceptability
SQEP	Suitably Qualified and Experienced Personnel
SSC	Structures, Systems and Components
SSER	Safety, Security and Environmental Reports
SSP	Site Security Plan
SSyC	Specific Security Claim
SVA	Security Vulnerability Assessment
SyAPs	Security Assessment Principles
TAC	Threat Actor Compromise
TAG	Technical Assessment Guide
TBC	To be Confirmed
UK	United Kingdom of Great Britain and Northern Ireland
URC	Unacceptable Radiological Consequence
VA	Vital Area
VAI	Vital Area Identification

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 10/46

2. Executive Summary

The Generic Security Report (GSR) is one of three submissions in the Generic Design Assessment (GDA) undertaken by The Office for Nuclear Regulation (ONR) and Environment Agency (EA) to assess the safety, security and environmental implications of new nuclear power station design. The process requires GNS on behalf of the Requesting Party (RP) to submit sufficient information to enable the Regulators to make an informed judgement on the adequacy of the safety, security and environmental aspects of the generic design, to support the construction and subsequent operation of the UK HPR1000 in the UK. At the end of the GDA process, subject to satisfactory design, the ONR will issue a Design Acceptance Confirmation (DAC) and the EA a Statement of Design Acceptability (SoDA).

General Nuclear System (GNS), on behalf of the Requesting Parties (RP), will submit a GSR V0 at the end of Step 2 and subsequent versions (V1, V2) in Steps 3 and 4 of the GDA, for assessment in support of achieving a Design Assessment Certification (DAC) by the ONR. The GSR will provide sufficient information to enable ONR to assess the key security claims and identify any fundamental shortfalls that could prevent ONR permitting the construction of a power station based on the UK HPR1000 design. In doing so GSR V0 and future versions will provide confidence to ONR that GNS understands the nuclear security risk relevant to the UK HPR1000 design and that such risks are adequately managed, ensuring they meet the relevant UK regulatory requirements.

Given the inherent nature of the GSR and the Design Basis Threat (DBT), GNS has established a Suitably Qualified and Experienced Personnel (SQEP) team to enable delivery of the GSR, accounting for the DBT and the revised regulatory environment the GSR will be developed within during the GDA process. Throughout the process China General Nuclear (CGN) as the HPR1000 reactor designer will work closely with the GNS GSR Team to provide the necessary reference information where applicable, however, the GSR will be produced in the UK by a UK based team.

GNS's intent is to deliver a product that is first and foremost fit for business need whilst providing sufficient information and detail to enable the ONR to assess the UK HPR1000 security submissions. This approach will enable GNS to establish a consistent approach to both the GSR and the future Nuclear Site Security Plan (NSSP) as it evolves through the project lifecycle: construction, commissioning, operations and decommissioning under the licensee. The methodologies presented are applicable throughout the lifespan of the UK HPR1000 and provide a true benefit to the licensee(s) ensuring a seamless

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 11/46

transition takes place at the end of the GDA process. As the GDA process develops and the GSR evolves, it is important that the future licensee is appraised of the GSR's direction. This approach will be reviewed throughout the GDA process, to ensure that as the GSR evolves, it meets the regulatory assessment requirements and business needs.

The regulatory environment within which the GSR is being undertaken, has developed considerably within the last two years as a consequence of the ONR introducing outcome focused regulation, via the application of Security Assessment Principles (SyAPs). The revised regulatory approach, focussed on outcomes, signifies a decisive shift away from prescription, with the emphasis on outcome focused security regulation. This approach should provide a coherent regulatory approach applied by ONR to both safety and security across the UK Civil Nuclear Industry (CNI). Outcome focused security regulation supports the regulatory aim of responsibility and ownership of civil nuclear security resting with duty holders. This enables duty holders to deliver against defined security outcomes, with ONR holding them to account.

Outcome focused regulation allows greater flexibility in approach and encourages innovation in security solutions. GNS is cognisant of the revised regulatory environment and the opportunities this potential affords the business. In order to maximise the benefits to the business of this operating environment, GNS is applying a Security Risk Management approach that utilises a logical and holistic 'threat driven', 'outcomes focused' approach, enabling GNS to fully articulate the resources to be protected, the threats, the linkage between the compromise method effects, the resultant business impacts and how the security regime security capabilities mitigate the security risks to acceptable levels. By adopting such an approach, this provides the basis for the business to make fully informed decisions, providing the means by which cost effective security solutions are developed, whilst describing the rationale for, and the nature of, the security regime required to meet the totality of the business needs and business threats, throughout the project life cycle of the relevant site.

The GSR relationship and integration with the Pre-Construction Safety Report (PCSR) and Pre-Construction Environmental Report (PCER) is critical to the success of the GDA. It is anticipated the identification and confirmation of VAs within the Vital Area Identification (VAI) process and Cyber Risk Assessment methodologies, the identification of security infrastructure design requirements, access control arrangements and development of the Concept of Operation (CONOP) will require significant safety case input and technical review where security may have an impact on safety, and vice versa. As a consequence, the approach to nuclear security recognises that the PCSR and PCER forms a key

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 12/46

baseline for the security assessments. Hence, where appropriate, reference will be made to the PCSR and PCER for source information both in terms of consistency of information across the project and efficiency.

In developing the GSR alongside the PCSR and PCER, it is recognised that there may be circumstances where security and safety requirements conflict. Management of this interface is achieved through an integrated approach to working between the security, safety and environmental teams including the use of cross cutting meetings and an integrated plant modification review process including periodic reviews of the cumulative effect of individual changes. In addition, where appropriate the GSR will utilise the common assessment framework adopted by GNS for optioneering and decision making across the UK HPR1000 GDA project, including the Design Organisation, which encompasses the four primary considerations of nuclear safety, environmental protection, conventional safety and security. The output of the optioneering and decision-making process will involve a decision regarding whether to enter the Modification Control Process with an agreed design change. Throughout the GDA process it is very important that safety and security considerations are understood to enhance safety and/or security, thereby ensuring that a fit for purpose UK HPR1000 GDA is delivered.

3. Public Release of Generic Security Report

The UK Regulatory framework is based on openness, transparency and public accountability. The GDA as a process is expected to be run in the spirit of that framework and in accordance with GNS legal responsibilities. During the project, GNS technical reports will be published on the UK GNS website and the UK Regulators responses are published on the ONR and EA GDA website. This will allow ease of access to information during the project and allow for the public to raise comments throughout the duration of the GDA to the appropriate body, in accordance with each organisations individual responsibilities under the Freedom of Information Act 2000.

Some information related to the design and operation of nuclear power plants is of a sensitive nature and can be subject to a high level of security classification. GNS whilst recognising the requirement for openness and transparency and public accountability, has a requirement to adhere to UK Information Security policies and relevant good practice such as Her Majesty's Government (HMG) Security Policy Framework and relevant Office for Nuclear Regulation (ONR) references including the management of Sensitive Nuclear Information and other classified material when managing information. In addition, some UK context reference material is also classified. This means that only UK nationals or foreign nationals with the pre-requisite residency criteria

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 13/46

and with appropriate National Security Vetting (NSV) clearance can access the GSR and classified reference/support material, for example the UK DBT. The control and management of SNI and any classified information is therefore imperative.

The GSR adopts a three-tiered approach with the GSR providing an overarching Tier 1 document providing a synopsis of key information contained within Tier 2 documents. The GSR will have annexes and appendices where appropriate. The GSR will be supported by Tier 2 documents covering key topic areas in detail specific to the GSR scope within GDA. Tier 3 documents are produced providing further levels of information and reference material relevant to the GSR and Tier 2 documents. It is anticipated that all documents at the various levels will evolve throughout the GDA process.

In accordance GNS responsibilities of adhering to UK Information Security policies, each annex, appendix and supporting Tier 1, 2 and 3 documents are classified and protectively marked based upon an assessment of the material contained within. Annexes, appendices and supporting documents are classified as either: NOT PROTECTIVELY MARKED, UK PROTECT, OFFICIAL-SENSITIVE: SNI and/or SECRET. Documents, annexes and/or appendices attracting a classification of UK PROTECT, OFFICIAL-SENSITIVE: SNI and/or SECRET will not be releasable and will not be available for public review. Readers should refer to section 18 'References' for confirmation as to the classification and protective marking of each document referenced within the GSR.

4. Introduction

The Generic Design Assessment (GDA) is a four-step process undertaken by the Office for Nuclear Regulation (ONR) and the Environment Agency (EA) to assess the safety, security and environmental implications of new nuclear power station design. The process requires GNS on behalf of the Requesting Party (RP) to submit sufficient information to enable the Regulators to make an informed judgement of the adequacy of the safety, security and environmental aspects of the generic design, to support the construction and subsequent operation of the UK HPR1000 in the UK. At the end of the GDA process, subject to the design being satisfactory, the respective external regulatory bodies will issue a Design Acceptance Confirmation (DAC) and a Statement of Design Acceptability (SoDA).

The Generic Security Report (GSR) is one of three submissions in GDA, the other two being the Pre-Construction Safety Report (PCSR) and the Pre-

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 14/46

Construction Environmental Report (PCER). As such the overarching Safety, Security and Environment Report (SSER) Delivery Strategy Reference [1] presents the general requirements and arrangements put in place to ensure the SSER are well managed in terms of quality, budget and delivery; specific detail for each submission is described in the respective strategy document.

The GSR will provide sufficient information to enable ONR to assess the key claims and identify any fundamental identify shortfalls that could prevent ONR permitting the construction of a power station based on the UK HPR1000 design. In doing so GSR V0 and future versions provide confidence to ONR that GNS understands the nuclear security risk relevant to the UK HPR1000 design and that such risks are adequately managed, meeting the relevant UK regulatory requirements. Adequate security documentation will be developed during Steps 3 and 4 for subsequent assessment.

Given the inherent nature of the GSR and the Design Basis Threat (DBT) Reference [3] GNS has established a Suitably Qualified and Experienced Personnel (SQEP) team comprising safety and engineering, Operational Technology (OT) and Information Technology (IT), threat analysis and operational security Subject Matter Expertise that will deliver the GSR. China General Nuclear (CGN) as the HPR1000 reactor designer will work closely with the GNS GSR Team to provide the necessary reference information where applicable, however, the GSR will be produced in the UK by a UK based team.

5. Generic Security Report (GSR) Route Map

The GSR is one of three submissions in the GDA, the other two being the PCSR and the PCER. The Safety, Security and Environment Report (SSER) provides the overarching general requirements and arrangements put in place to ensure the three respective topic areas are well managed in terms of quality, budget and delivery.

The GSR adopts a three-tiered approach with the GSR providing an overarching Tier 1 document providing a synopsis of key information contained within Tier 2 documents. The GSR will have annexes and appendices where appropriate. The GSR will be supported by Tier 2 documents covering key topic areas in detail specific to the GSR scope within GDA. Tier 3 documents are produced providing further levels of information and reference material relevant to the GSR and Tier 2 documents. It is anticipated that all documents at the various levels will evolve throughout the GDA process. The present document set supporting GSR V0 consists of:

- Tier 1: GSR V0 (NOT PROTECTIVELY MARKED);

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 15/46

- Annex A – Acronyms & Definitions (UK PROTECT).
- Tier 2:
 - Security Case (UK PROTECT);
 - Security Risk Management Approach (UK PROTECT);
 - Annex A – Security Case Step 2 Route Map (UK PROTECT);
 - Annex B – Step 2 Security Case Arguments Table (UK PROTECT).
 - Vital Area Identification Methodology (UK PROTECT);
 - Annex A – VAI Methodology flow chart (UK PROTECT).
 - Plant Design and Information Report;
 - Annex A – Plant Information (UK PROTECT).
 - GSR Definitions (UK PROTECT);
- Tier 3:
 - NM/ORM Inventory (UK PROTECT);
 - Step 2 Identified Operational Technology (UK PROTECT);
 - Tier 3 Document titled GSR ONR/GNS Guidance Reference Matrix (UK PROTECT).

In line with the development of the GSR it is expected that additional Tier 2 and 3 documents will be developed in Steps 2 and 3 of the GDA.

6. General Nuclear System (GNS) Approach to GDA

6.1 General

GNS has been established to deliver the GDA for the HPR1000 Technology, which will establish a UK HPR1000 generic design. GDA enables the safety, security and environmental implications of new nuclear power station designs to be assessed before applications are made for the permissions required to build that design at a particular site. The nuclear regulator, the ONR and the Environment Agency, undertakes the GDA process.

Upon successful completion of the GDA process the ONR and the Environment Agency (EA) (the Regulators) will issue acceptance certificates for the UK HPR 1000 design. This will allow the design to be considered for Licensing at a UK site. GNS plans to deliver the GDA within a schedule capped at 60 months (from formal GDA entry). Upon completion of the GDA, knowledge of the project will be transferred to the future licensee thereby ensuring no loss of corporate knowledge of how the design has evolved from the reference plant (Fangchenggang Unit 3 HPR1000) into the UK HPR1000 design.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 16/46

The process associated with the delivery of a GDA is well documented in the regulatory guidance; the strategy to deliver the process is up to the Requesting Party (RP) to decide. The Requesting Parties (RPs) for the purpose of the UK HPR 1000 GDA process are constituted jointly by China General Nuclear Power Corporation (CGN), Électricité de France (EDF S.A.) and General Nuclear International (GNI). GNS is appointed by the above RPs and has delegated authority to make decisions in respect of the GDA business, including in respect of any matters that are the responsibility of the RP. The strategy for the GDA will be developed over the duration of the GDA and will remain flexible while focused on reducing the risks for the licensing phase.

6.2 GDA Scope

GDA is a flexible project that allows the separation of design issues from specific site related issues, which is likely to be beneficial where the generic design is intended for construction on a number of different sites. It is the responsibility of the GDA organisation to strategically decide how specific or generic the GDA will be. One of the key strategy documents that has been developed relates to the scope of the GDA Reference [4]. This strategy document defines the boundaries of the work to be delivered during the GDA and the key assumptions made to define this scope. It also defines the Generic Site Characteristics and Envelope that will be used for the GDA and therefore the potential site or sites the UK HPR1000 will be built at.

The current intended site for the UK HPR1000 is Bradwell in Essex, however the Generic Site Characteristics and Envelope establish the parameters and values chosen for the GDA. The total scope of the UK HPR1000 project is much broader than that of the GDA and this will be covered appropriately by the future licensee. The aim is to take the HPR1000 reactor design through GDA, licensing, construction, commissioning and on into safe reliable operation. GNS as an organisation exists to deliver the GDA associated with this project, this phase will take 60 months to deliver with subsequent phases occurring over the next decade or so.

6.3 GNS The Organisations

The GNS Shareholder Agreement provides a full specification of all the governance structures and decision-making processes for the GDA. The project management and technical arm of the organisation is based on a structured hierarchy from the Executive through the Lead Project Correspondents (PCs) through which the GDA will be delivered. GNS is the point of contact for all regulatory interaction in the UK and has been designed to allow tiered interaction.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 17/46

The operating model for GNS is one of technical project delivery operating as the technical project engineers integrating the design information and the safety case to make sure it is fit for purpose for the UK Regulatory regime. In the shareholder agreements (Classified as Proprietary and non-releasable) signed between the parent companies, technical support and resource is guaranteed by those companies for the delivery of the GDA. The specifics of the types of service are defined in the Framework Service Contract agreement (Classified as Proprietary and non-releasable) between GNS / CGN and GNS / EDF and against which work is specified through task orders and work delivery plans developed collaboratively between GNS and its service providers. Sufficient competencies are held within GNS to specify technical work and (with the support of a third party if needed) receive it back into the organisation. GNS will be supported throughout the delivery of the GDA and should not be considered in isolation in terms of its technical competency.

6.4 Lead Project Correspondents

Lead Project Correspondents (PCs) are the primary means through which the GDA and specific topic areas are managed and delivered. Lead PCs work collaboratively across topic areas as a team to make sure there is visibility of cross cutting issues across the whole GDA project team. Accountability for cross cutting issues sits formally with the Design Lead PCs as a discrete topic, however it is the responsibility of all the Lead PCs to raise issues, manage aspects of cross cutting issues, and maintain visibility of problems.

The Lead PC security is responsible for the project and technical management of the GSR, utilising the GNS governance arrangements to manage delivery. The Lead PC Security will be the lead for technical interface with the regulators and any service providers who support the security work stream and GSR delivery. Quality management of the processes to deliver GSR is the responsibility of the Lead PC Security. The Lead PC is also the Departmental Security Office (DSO) and Chief Information Security Officer (CISO) for GNS. The lead security PC is directly supported by Information Security PC and team of external third party suppliers, providing Subject Matter Expertise.

6.5 Third Party Service Provision

Provision has been made for GNS and Lead Project Correspondents in delivery of the GDA to utilise the supply chain for 3rd party service provision. A balanced and proportionate approach has and will continue to be taken through the stages of the project to develop the organisations capabilities up to the point GNS transitions into the Licensing organisation that will be defined in future years. This is aimed to build solid foundations upon which knowledge acquired through the project is effectively managed and maintained into the

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 18/46

future.

6.6 Governance

The GNS organisation is empowered by the shareholders (and requesting parties) to manage the day to day business of delivering the GDA. The interactions between the GNS Board, the Executive Committee and the staff delivering the GDA are frequent and managed via a series of structured meetings to make sure that there is clear line of sight on progress, risks and deviation from the programme declared to the UK regulators.

7. General Nuclear System (GNS) – The GDA Process

GNS plans to deliver the GDA within a schedule of 60 months (from formal GDA entry). The duration of the four GDA steps have been defined in the Level 1 milestones of the GDA Schedule Plan Reference [18] and approved by the GNS board of GNS:

- Step 1 – 10 months;
- Step 2 – 12 months;
- Step 3 – 13 months;
- Step 4 – 25 months.

The Work Plan for GDA is based upon GDA Entry in January 2017 with project duration of 60 months resulting in a DAC and SoDA in January 2022. It is the intention of GNS to manage the work to achieve a successful project through rigorous planning and to establish clear accountability in all three partners (GNS, CGN, and EDF). The overall GDA Level 1 program is based on a total project duration of 60 months, which is broken into 4 Steps that run in series as required by ONR and EA guidance.

T-7-1 GDA Duration

GDA Step	Duration (months)	Key Document Submissions (at end of step)
1	10	Preliminary Safety Report (PSR)
2	12	Pre-Construction Safety Report (PCSR) Pre-Construction Environment Report (PCER) Generic Security Report (GSR) All at version 0
3	13	PCSR, PCER, GSR (version 1)
4	25	PCSR, PCER, GSR (version 2)

To present the GSR in context, the GDA process is briefly outlined:

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 19/46

- Step 1 was the preparatory part of the design assessment process. The step involved the RP establishing its project management and technical teams and arrangements for GDA, and writing and preparing submissions for Step 2, including the PSR. Within Step 1 the GSR primary aim was to put in place the strategic security enablers facilitating entry into Step 2 whilst setting the conditions for Step 2 delivery;
- Step 2 is an overview (by ONR and EA) of the acceptability, in accordance with the UK regulatory regime, of the design fundamentals, including review of key safety and security claims. Step 2 of the GDA process requires the RPs to submit a SSER providing an outline description of the reactor equipment and structures, the design and safety philosophy, the codes and standards applied in the design and the quality management systems applied by the designers. The aim is to give the ONR and EA confidence that UK safety standards could be met by the proposed reactor design and that the claimed principles and design criteria are likely to be achievable. Within Step 2, the GSR primary aim is to:
 - Develop an understanding to the UK HPR1000 plant and design;
 - Define GNS' approach to GDA scope and the GSR's strategy Reference [2] acknowledging the wider approach to the security spectrum outside of GDA scope;
 - Develop GNS' Security Risk Management methodology, including:
 - Methodology for the identification of Vital Areas (VAs);
 - Cyber Risk Assessment methodology.
 - Develop a Security case against which RP's claims within step 3 regarding the safety and related security aspects of the proposed design will be reviewed;
 - Define GNS' proposed approach to developing the security regime operation Concept of Operation (CONOP).
- Step 3 is the period the ONR will review the arguments supporting the RP's claims regarding the safety and related security aspects of the proposed design. The intention in this step is to move from the fundamentals of the previous step to an analysis of the design, primarily by examination at the system level and by analysis of the RP's arguments that support the safety and security claims. Within Step 3 of the GDA, the GSR primary aim will be to:
 - Development of Security Case;
 - Continue to develop an understanding of the UK HPR1000 design;

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 20/46

- Identification of opportunities to inform the UK HPR 1000 design; security by design;
 - Identification of security infrastructure design requirements;
 - Apply the Security Risk Management approach (SRMA) Reference [14], including enabling the identification and categorisation of UK HPR1000 VAs;
 - Identify ONR Security Outcomes;
 - Develop the security regime operation CONOP in further detail in support of the UK HPR1000 Security Regime;
 - Identify access control arrangements;
 - Development of plot plans showing access routes, emergency routes, doors etc. relative to those areas containing VAs and CBSIS etc;
 - Develop Plot plans detailing CBSIS not in VA locations.
- Step 4 is an in-depth assessment of the safety case evidence, security case evidence and the generic site envelope. The general intention of this step is to move from the safety arguments and system level assessment of Step 3 to a fully detailed examination of the available evidence, on a sampling basis, given in the safety and security submissions. Given the evolutionary nature of the GDA process, it is anticipated that the design and safety case will not be complete at the end of step 3, so step 4 will involve review and revision (as required) of the GSR relative to changes in the design and safety of the UK HPR 1000.

8. General Nuclear System (GNS) Approach to GSR

GNS's intent is to deliver a product that is first and foremost fit for business need whilst providing sufficient information and detail to enable the ONR to assess the UK HPR1000 security submissions to ultimately support the issue of a DAC at the end of Step 4 of the GDA process. This approach will enable GNS through the GSR to establish a consistent approach to both the GSR and the future Nuclear Site Security Plan (NSSP), which will be developed and delivered by the future licensee, as it evolves through the project lifecycle: construction, commissioning, operations and decommissioning under the licensee.

The methodologies presented are applicable throughout the lifespan of the UK HPR1000 and as such the final GSR V2 will be a more detailed product that is expected to meet regulatory assessment requirements. This is a conscious business decision that will be reviewed as the GSR evolves and will require

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 21/46

significant management to ensure that regulatory assessment requirements are first and foremost met. This approach will provide true benefit to the licensee(s) ensuring a seamless transition takes place at the end of the GDA process. As such it is imperative that as the GSR evolves that the future licensee is appraised of the GSR's direction and level of detail in order to ensure the licensee understands the approach expected to be inherited and the innovation therein.

The regulatory environment has significantly transformed within the last 18 months as a consequence of the ONR introducing outcome focused regulation, via the application of Security Assessment Principles (SyAPs). The revised regulatory philosophy represents a pivotal shift away from proscription and is aligned with the mature and non-proscriptive approach adopted in the regulation of the nuclear safety regime, providing duty holders with a coherent regulatory approach applied by ONR to both safety and security across the UK Civil Nuclear Industry (CNI). Outcome focused security regulation supports the regulatory aim of responsibility and ownership of civil nuclear security resting with duty holders. This enables duty holders and RPs to deliver against defined security outcomes, with ONR holding them to account for said delivery. Outcome focused regulation allows greater flexibility in approach and encourages innovation in security solutions.

GNS has entered into the GDA process; cognisant of the revised operating environment and the opportunities these conditions provide the future site licensee (herein referred to as licensee). GNS also recognises its obligations to meet the defined outcomes within GDA and its ultimate responsibility to the licensee, setting the conditions for their future success. GNS embraces this opportunity and is adopting an approach to the GSR, which will enable the business to meet the GDA's requirements, whilst identifying the full spectrum of security risks the licensee is likely to face. This is achieved by applying a Security Risk Management Approach (SRMA) that utilises a logical and holistic 'threat driven', 'outcomes focused' approach, enabling GNS to fully articulate the resources to be protected, the threats, the linkage between the compromise method effects, the resultant business impacts and how the security regime security capabilities mitigate the security risks to acceptable levels.

By adopting such an approach, this provides the basis for the business to make fully informed decisions, providing the means by which cost effective security solutions are developed, whilst describing the rationale for, and the nature of, the security regime required to meet the totality of the business needs and business threats, throughout the project life cycle of the relevant site. These include the specified ONR regulatory requirements and recognises other non-

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 22/46

regulatory requirements as necessary. It also provides the mechanism by which the security claims can be justified and are supported by the arguments and evidence ensuring the benefits are realised whilst demonstrating that the Security Regime is fully 'fit for purpose' against the business' risk appetite and ONR (CNS) requirements. GNS will leverage its collective expertise to ensure the alignment and optimisation of nuclear safety and nuclear security, thereby creating an integrated approach, providing the basis for the development of a proportionate, flexible and sustainable nuclear security regime.

Notwithstanding the wider benefits the approach confers, GNS' primary focus, at the end of the GDA process, subject to the design being satisfactory, is for the respective external regulatory bodies to issue a DAC and a SoDA. The GSR will provide sufficient information to enable ONR to assess the key claims and identify any fundamental security shortfalls that could prevent ONR permitting the construction of a power station based on the UK HPR1000 design. In doing so GSR V0 will provide confidence to ONR that GNS understands the nuclear security regulatory requirements for the UK and that adequate security documentation will be developed during Steps 3 and 4 for subsequent assessment. Given the nature of this GDA GNS and the GSR team have the ability to call upon the Joint Venture parties of CGN, the HPR1000 reactor designer and EDF Energy (EDF) for relevant Operational Experience (OPEX).

9. GNS Approach to Regulation and Reference Material

As indicated within Section 7, the regulatory environment within which the GSR is being delivered has significantly developed within the last 18 months as a consequence of the ONR introducing outcome focused regulation, via the application of Security Assessment Principles (SyAPs). Given the revised regulatory approach, with the emphasise on outcomes and the responsibility and ownership of civil nuclear security resting with duty holders, this enables duty holders and RPs to deliver against defined security outcomes, with ONR holding them to account for said delivery. As a consequence, outcome focused regulation allows greater flexibility in approach and encourages innovation in security solutions.

Given these changes, GNS embraces this opportunity and is adopting an approach to the GSR, which will enable the business to meet the GDA's requirements, whilst meeting the respective external regulatory bodies requirements. In line with this approach, GNS has undertaken a review and will continue to do so, of ONR guidance and reference material to ensure that the GSR meets the regulatory bodies requirements, with the GSR and supporting documents, providing the mechanism by which the security claims can be

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 23/46

justified and are supported by the arguments and evidence.

The Tier 3 Document titled GSR ONR/GNS Guidance Reference Matrix outlines the identified ONR guidance and reference material and the associated requirements and expectations therein. The matrix will be used to clearly identify where in the GSR such requirements, expectations and/or guidance are addressed be it in the form of a claim, sub-claim, argument or supporting evidence thereby providing a baseline record for GNS and licensee(s) to reference as well as clear ownership should any elements be referred out to the licensee. In doing so the matrix will provide clarity for the ONR's assessment as the GSR matures. This document will remain an extant Tier 3 Document of the GSR that will evolve through future iterations. Comments or questions relating to the GSR assessment by ONR (CNS), should be directed to the ONR (CNS).

9.1 Security Assessment Principals (SyAPs)

GNS recognises the revised approach to regulation through the ONR application of the SyAPs Reference [6]. SyAPs provide the essential foundation for the introduction of outcome focussed regulation with outcome focussed security regulation providing clarity that responsibility for ownership and control of civil nuclear security rests with duty holders. The primary purpose of the SyAPs is to provide ONR with a framework for making consistent regulatory judgements on the adequacy of security arrangements. Although it is not their primary purpose, the SyAPs may also provide guidance to designers and duty holders on the appropriate content of security plans, clarifying our expectations in this regard.

The fundamental principles in SyAPs enable the duty holders to deliver the defined security outcomes, with ONR holding them to account for that delivery. Outcome focussed regulation allows greater flexibility in approach and encourages innovation in security solutions that provide effective and robust protection against the modern threat environment, whilst working in harmony with business processes and maximising opportunities for adding value. The SyAPs support this flexibility enabling alternative approaches to those defined in the fundamental principles to be applied when justified.

However, SyAPs are not sufficient on their own to be used as design or operational standards, nor are they intended for that purpose, requiring parties to draw upon Relevant Good Practice (RGP) and external codes and standards to inform their approach. Where appropriate and in line security analysis requiring an extensive understanding of the facility and its safety case, both in the present and foreseeable future, the GSR will draw upon relevant regulatory

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 24/46

material relating to Safety, contained within the ONR Safety Assessment Principles (SAPs). Comments or questions relating to the SyAPs and/or SAPs should be directed to the ONR (CNS).

9.2 ONR CNS Assessment Plans

The ONR's GDA process calls for a step-wise assessment of the RP's security submission with the assessments becoming increasingly detailed as the project progresses. The Step 2 Assessment Plan for Security by the ONR (CNS) Assessor sets out the key assessment activities to be undertaken upon submission of GSR V0, with subsequent assessment plans produced by ONR supporting Step 3 and 4 of the GDA. Questions relating to ONR (CNS) Assessment Plan should be directed to the ONR.

9.3 ONR Technical Meetings

The Level 4 Technical meetings between GNS and the ONR provide a formal forum and means for technical exchange; the opportunity for ONR to clarify requirements and expectations specific to the reactor design during the course of their assessment and to involve CGN as the reactor designer where applicable. To date no additional ONR security requirements or expectations have been identified during meetings between the RP and ONR on the GDA for the UK HPR1000. Questions relating to ONR (CNS) technical meetings should be directed to the ONR (CNS).

9.4 Regulatory Queries (RQs), Regulatory Observations (ROs), Regulatory Issues (RIs)

RQs, ROs and RIs provide a means by which ONR clarify requirements and expectations or raise questions or comments specific to the reactor design during the course of their assessment. ONR issued two RQs specific to the PSR, Chapter 27 (Security) during Step 1, these RQs were closed during Step 1. To date no further RQs have been issued nor have any ROs or RIs been issued during the production of the GSR. Future RQs, ROs and RIs if issued will be managed between the GNS GSR Team and CGN (where applicable) and the ONR. Questions relating to Regulatory Queries (RQs), Regulatory Observations (ROs), Regulatory Issues (RIs) should be directed to the ONR (CNS).

9.5 Relevant Good Practice

The GSR will use RGP material where appropriate, such as International Electro-technical Commission (IEC), International Atomic Energy Agency (IAEA), ONR guidance and reference material and Department of Homeland Security (USA) in development of the GSR.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 25/46

9.6 Suitably Qualified Experienced Persons

In accordance with a key regulatory requirement, GNS has established a SQEP team comprising safety and engineering, Operational Technology (OT) and Information Technology (IT), threat analysis and operational security Subject Matter Expertise (SME) that will deliver the GSR. All personnel have the appropriate UK National Security Vetting (NSV) and clearances.

10. Terminology¹

The GSR contains safety and security terminology. As such much of the security terminology, and in some cases safety terminology, will be new to readers and it is important that Annex A (GSR Definitions & Acronyms) is used in parallel when reading the GSR. This Annex will evolve as the GSR evolves.

11. Interactions with Others

The development of the GSR during the GDA will require interaction with a broad range of stakeholders, including within CGN (as the reactor designers), GNS (as the RP), the regulators, EDF Energy, BRB (as the licensee) and the public, as addressed in this section.

11.1 UK HPR 1000 CGN/GNS SMEs

The interaction with CGN and GNS is aimed at:

- Delivering a security informed design for the UK HPR1000;
- Delivering an optimum design for the UK HPR1000;
- Delivering a GSR which is consistent with the PCSR and PCER for the UK HPR1000;

The interaction with CGN and GNS will be on going throughout the GDA.

11.1.1 Security Informed Design

The opportunity to security inform design will be an on going process during the development of the GSR, from the identification of assets for protection to the development of the conceptual security arrangements and security regime, as noted in previous sections of GSR V0.

It will be an objective of the UK security team during all stages of the GSR development, but in particular during Step 3, to identify potential opportunities to inform the design based on a design hierarchy of controls in order to 'reduce

¹ It is recommended that the reader uses Annex A whilst reading the GSR

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 26/46

the need and reliance on protective security systems, and the challenges placed on them' as per the SyAPs Reference [6].

Potential design changes identified by the security team will be progressed at the earliest opportunity through the UK HPR1000 Design Control Strategy Reference [8].

It is noted that during the course of the GDA, there will be potential design changes identified by others. There will be security team representation in the consideration of these design changes so that the impact of those changes to the nuclear security case is understood and taken into account in assessment and selection of the appropriate design change solution. This will include representation via the:

- UK HPR1000 Design Control Strategy, Reference [8];
- UK HPR1000 Requirements on Optioneering and Decision Making, Reference [9];
- UK HPR1000 Modification Control Procedure, Reference [10];
- UK HPR1000 Technical Committee Operation Guidance, Reference [11];
- UK HPR1000 Cross Cutting Forum Terms of Reference, Reference [12].

11.1.2 Optimum Design for the UK HPR1000

Security informed design also facilitates the delivery of an integrated and optimised design for the UK HPR1000 by:

- Benefiting on the opportunities to be gained when the security and safety requirements are consistent;
- De-conflicting possible opposing requirements between security and safety.

This will require close working arrangements with CGN/GNS SMEs during Steps 3 and 4. This will be achieved via:

- Frequent informal interaction, as required, between the UK security team and the CGN/GNS SMEs (See section 1.1.3 below);
- The UK HPR1000 Cross Cutting Forum, Reference [12];
- Workshops between security team and CGN/GNS SMEs on specific topics.

11.1.3 Consistency with PCSR and PCER

The development of the nuclear security case and security arrangements for the UK HPR1000 will require input from the PCSR, PCER, and the design and

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 27/46

layout for the plant, including in particular in the following functional areas:

- Site Layout and Internal Building Layouts;
- Nuclear Inventory;
- Safety Case, in particular:
 - External Hazards;
 - Internal Hazards;
 - Fault Studies;
 - PSA;
 - Radiation Protection;
 - Operation and Maintenance;
 - Human Factors;
 - Nuclear and Conventional Fire.
- Design, in particular:
 - Fuel and Core;
 - Civil and Structural;
 - I&C Design;
 - Electrical;
 - Radioactive Waste.
- Operations.

It is important that this input is consistent with the information being developed by the CGN/GNS SMEs in these functional areas for the GDA.

This will be achieved via a combination of:

- Frequent informal interaction, as required, between the GSR UK based security team and the CGN/GNS SMEs;
- The UK HPR1000 Cross Cutting Forum, Reference [12];
- Obtaining text/data from the CGN/GNS SMEs for direct inclusion in the GSR;
- The review of text/data in the GSR by CGN/GNS SMEs;
- Workshops between security team and CGN/GNS SMEs on specific topics.

11.2 CGN Physical Protection Group

The UK HPR is based on the Fangchenggang nuclear power plant Unit 3 (FCG3). China General Nuclear Power Company (CGN) has conducted a nuclear security assessment of FCG3 compliant with Chinese nuclear security regulations that has been reviewed and approved by the National Nuclear Safety Administration (NNSA). This assessment will contain nuclear security information on the FCG3 that would be beneficial for the derivation of the security arrangements of the UK HPR1000. To this end, it is expected that there will be interaction with the Physical Protection Group from CGN.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 28/46

11.3 Regulators

11.3.1 ONR

Interactions with ONR will be as per the ONR Assessment Plan and as agreed with the GNS GDA Project Management Team. This interaction is expected to include during Steps 3:

- Workshops;
- Level 4 Technical meetings and workshops;
- Progress Teleconferences.

11.3.2 EA

Whilst the EA is a stakeholder, no specific interaction is currently expected with EA during Step 3.

11.4 BRB

As a prospective licensee for the UK HPR1000, there will be regular interaction BRB during Step 3 with the dual aim of:

- Keeping BRB informed of developments with the GSR and expectations being placed upon them by the GDA;
- Appraising the GDA security team of BRB operational requirements.

This will be to ensure a seamless adoption of the GSR and transfer from GDA to site specific licensing.

11.5 Public

Interaction with the public will be via the UK HPR1000 GDA website.

12. UK HPR Plant Information

The following section is a summary of the plant information contained within the Design & Plant Information Report Reference [7] that focuses on those aspects that are important to the development of the GSR. The Design & Plant Information Report uses the PCSR and PCER as its principal references. These provide the complete details of the UK HPR1000 design as published at this stage in the plant development.

12.1 Introduction to UK HPR1000

The reference design for the UK HPR1000 is the Hualong Pressurised Reactor currently under construction at Fangchenggang Unit 3 in southern China. This represents an evolutionary design of a three loop Pressurised Water Reactor (PWR) based technology systematically modified and developed based on

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 30/46

Access to the nuclear island for personnel and equipment is facilitated by the Personnel Access Building (BPX) and Equipment Access Building (BEX) respectively.

Three EDG Buildings (BDA/BDB/BDC) and two SBO Diesel Generator Buildings (BDU/BDV) are provided which form two clusters of buildings, which are separately arranged, on either side of BRX. One group of buildings includes two EDG Buildings (BDA and BDC) and one SBO Diesel Generator Building (BDU), another group consists of one EDG building (BDB) and one SBO Diesel Generator Building (BDV).

The Extra Cooling System and Fire-fighting System Building (BEJ) is located adjacent to BFX and houses the Extra Cooling System (ECS [ECS]) and the Fire-fighting Water Production System (JAC [FWPS]), providing for the removal of core residual heat and decay heat from spent fuel under total loss of cooling or station black out scenarios

The Conventional Island principally comprises the Turbine Generator Building (BMX), Conventional Island Electrical Building (BLX), Main Unit Transformer and Auxiliary Transformer Platform (BTA), Backup Transformer Platform (BTX) and Standby Transformer Platform (BJX).

The Plant Design and Information Report Reference [7] provides a more detailed introduction to the UK HPR1000 plant design, layout and operating processes, including:

- Site Layout and Main Buildings;
- Characteristics of Civil Structures;
- Descriptions of Key Plant;
- Key Specifications;
- Fundamental Safety Functions;
- Operating Modes;
- Fuel Route Operations;
- Radioactive Waste Management;
- Systems within GDA scope;
- Operational Technology (CBSIS).

12.2 Use of Plant Information

The Plant Design & Information Report outlines how plant information (including the PCSR, PCER, supporting analyses, design information and layout drawings)

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 31/46

will be used within the nuclear security assessments, including identification of VAs, as well as presenting an overview of the processes in place to ensure that design modifications are security-informed.

13. GNS Security Risk Management Approach

13.1 Introduction to Security Risk Management Approach

The transition from National Objectives, Requirements & Model Standards (NORMS) Reference [13] SyAPs Reference [6] as the means by which the ONR Regulates the nuclear industry, has resulted in the industry moving from a proscriptive security approach to a goal-orientated security approach. Whilst this transition means that industry now has greater scope in deciding how security is delivered, industry must now be better able to describe the security that is in place and, importantly, justify how such security ensures that the ONR regulated security outcomes are met. This justification need means that GNS will utilise a security risk management approach in support of the design for the UK HPR1000 that is holistic and systemic in identifying the threats facing the future licensee and the security capabilities that the future licensee may utilise to mitigate such threats to acceptable levels for the UK HPR1000. This security risk management approach is presented through the utilisation of a security regime model.

This approach is defined within a tier two document HPRGDAREPO0060 - GNS - Security Risk Management Approach Reference [14] that supports the production of the GSR-V0. The classification of the document is UK PROTECT and as such is not releasable into the public domain. The purpose of the document is to present the security risk management approach, in the form of a GNS security regime model, which has been utilised during the GDA process as the basis for formulating the VAI methodology and will be utilised during the implementation of the VAI methodology for the UK HPR1000. This security risk management approach also provides the framework in which the security regime operation CONOP for the UK HPR1000 will be formulated.

Whilst the key requirement to be met by GNS during GDA is the identification and implementation of the VAI methodology for the UK HPR1000, - in order to be able to provide the basis for the production of the security regime operation CONOP and ensure continuity between GNS and the future licensee, the security regime model has been developed to provide the means to:

- Holistically identify and articulate the physical and cyber threats to the

future licensee’s resources and the components of the threats; including those regulated through ONR and other statutory bodies, and other business threats;

- Holistically identify, articulate and justify the physical, digital and personnel security capabilities, and the components of the security capabilities, selected to mitigate the threats to acceptable levels i.e. the ONR security outcomes or against the future licensee’s risk appetite.

13.2 Security Regime Model

The security regime model in support of the UKHPR1000 design will be utilised to ensure a consistent approach is taken to identifying and articulating physical and cyber threats; and identifying, articulating and justifying security capabilities. In the case of cyber risk assessment this will be in combination with recognised cyber security risk assessment standards that will or may be utilised during and after GDA.

The Security Regime model consists of a threat operation component and a Security Regime Operation component, as illustrated conceptually in Figure 1.

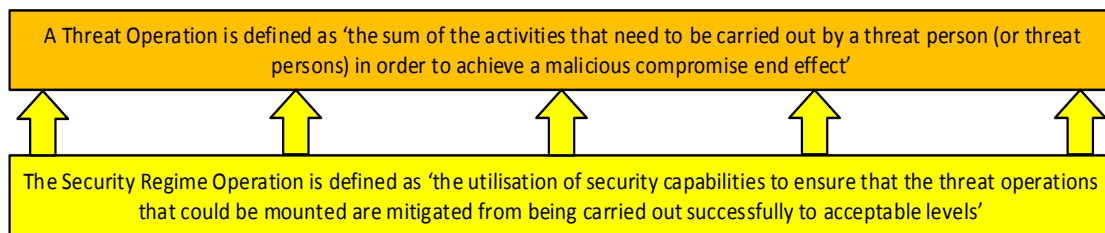


Figure 2: Security Regime Model

The Security Regime model is utilised to inform the definition of security requirements and the subsequent design of the Security Regime Operation in support of the UK HPR1000, and forms the basis for justifying and presenting that the Security Regime Operation is fit-for-purpose.

13.3 Benefits of Approach

The additional benefits from utilising the Security Regime model as the basis for the security risk management approach in support of the UK HPR 1000 design assessment include providing the means:

- By which Security Vulnerability Assessments (SVAs) can be carried out and documented, either as generic bounded SVAs or specific threat SVAs;
- To ensure assertions without supporting evidence are minimised;

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 33/46

- To ensure that where Operational Experience (OPEX) is utilised in support of arguments, the relevance is substantiated by SQEP;
- By which informed stakeholder engagement, including internal and external assurance, can take place by utilising a consistent and logical end-to-end 'golden thread' approach;
- Against which security claims, arguments and evidence can be formulated and presented;
- To better accommodate change including to the security regime operation as and when required.

14. Vital Area Identification Methodology

A critical requirement within the scope of the Generic Security Report (GSR) is to identify and categorise Vital Areas (VAs) against sabotage. Step 2 of the UK HPR1000 Generic Design Assessment (GDA) requires the submission of Vital Area Identification (VAI) methodology to the nuclear security regulators within the ONR (CNS). The Vital Area Identification (VAI) methodology is a Tier 2 document produced in support of the GSR V0. The VAI methodology is defined within HPRGDAREPO0062 – Vital Area Identification Methodology Reference [15]. The classification of the document is UK PROTECT and as such is not releasable into the public domain. The purpose of the document is to provide an explanation of the methodology utilised to identify and categorise VAs within the scope of GDA. The Scope for UK HPR1000 GDA Project is defined within Reference [4].

The VAI methodology provides details on the following:

- The methodology supporting the Identification of Nuclear Material/ Other Radiological Material (ORM) and the identification of potential target combination a, including potential targets relating to Computer Based Systems Important to Safety (CBSIS);
- The process supporting the assessment of threats;
- The means by which credible threats are derived, supporting the identification and categorisation of VAs;
- The means by which credible CBSIS targets are identified and the links to the VAI methodology.

The VAI methodology is informed by the 'Security Risk Management Approach Reference [14] utilised by GNS to identify and articulate the physical and cyber threats and components of the threats within scope of GDA relevant to UK HPR1000. The VAI methodology is also informed by the Plant Design &

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 34/46

Information document, General Nuclear System - Plant Design & Information Report Reference [7]. Where appropriate, the VAI methodology utilises GNS processes and guidance to support its delivery.

GNS has developed a suitable VAI methodology that provides the means to identify Unacceptable Radiological Consequence (URC) based threats. The requirement to identify URC based threats is covered by the Specific Threat Claim within the Security Case Report Reference [16]. See section 14 for details on the GNS approach to the Security Case. GNS recognises that throughout the GDA process, the VAI methodology will need to accommodate for change, whether that be changes in the DBT or changes in the design of UK HPR1000.

14.1 VAI Methodology Overview

The VAI methodology has been divided into five phases:

- Phase 1 - The Identification of NM & ORM;
- Phase 2 - The Identification of Potential Target combinations;
- Phase 3 - Assessment of Threat;
- Phase 4 - Identification of Credible threats;
- Phase 5 - The Identification and Categorisation of Vital Areas (VAs).

The VAI methodology, including the Cyber Risk Assessment methodology is consistent with the outcomes required from the application of a VAI methodology as defined within 'ONR Nuclear Safety Technical Assessment Guide, Target Identification for Sabotage, CNS-TASTGD - 6.2, Rev. 0, March 2017 Reference [17]. The VAI methodology has been developed utilising SQEP experience from the EDF Energy NG operating fleet and wider industry, Operational Experience (OPEX) and Relevant Good Practice (RGP) where appropriate.

14.2 Cyber Risk Assessment Methodology

The Cyber Risk Assessment Methodology utilised in support Vital Area Identification (VAI) is limited to identifying Computer Based Systems Important to Safety (CBSIS). The classification of the document is UK PROTECT and as such is not releasable into the public domain. The Cyber Risk Assessment Methodology is defined within Vital Area Identification Methodology Reference [15]. Computer Based Security Systems (CBSy) and Information Technology (IT) are to be considered separately at the enterprise level. It is assumed the assessments of CBSy and IT will align with and potentially use relevant standards such as ISO 27001 or similar.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 35/46

14.2.1 Methodology Overview

The following steps provide a high-level description for each Step undertaken during the Cyber Risk methodology. The output from Step 7 provides a list of potential Operational Targets incorporated into the outputs from Phase 2 – Identification of Potential Targets within the VAI Process.

- Step 1 - Obtain a list of CBSIS that falls within the GDA Scope;
- Step 2 - Consider which cyber-related standards these CBSIS have been assessed against;
- Step 3 - Conduct a review to determine which systems will result in a URC either directly or indirectly. Incorporating the initial steps of the VAI process to identify the potential CSSCs;
- Step 4 - Conduct a Cyber Risk assessment;
- Step 5 - Conduct change management process;
- Step 6 - Deliver potential targets to be assessed against National DBT;
- Step 7 - Protection of CBSIS.

As part of the assessment, a basic assumption has been made that the life cycle of Computer Based Systems will have security inherent in their design, these include; IT, OT (CBSIS, CBSy) and NMAC. However, this assumption is not made for Basic Process Control & Instrumentation Systems (BPC&I). These assumptions will be confirmed during the GDA cyber assessment.

15. GSR Security Case

15.1 General

The transition from NORMS Reference [13] to SyAPs Reference [6] as outlined within Section 8, provides the opportunity for the security function to better align itself to the proven design approach utilised by the safety function within the GDA process that is based on a hierarchy of objectives, claims and arguments. GNS has therefore produced a suite of threat and security-based claims and arguments which are presented within a hierarchal approach within the SSER route map under the single GNS GDA Fundamental Objective.

This security case is defined within the Security Case Report Reference [16], which is a Tier 2 document produced in support of the Generic Security Report (GSR) V0. The classification of the document is UK PROTECT and as such is not releasable into the public domain. The security case should be read in combination with the Security Risk Management Approach Reference [14], both of which provide the framework under which the VAI Methodology Reference

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 36/46

[15] sits; whilst also providing the umbrella under which the Security Regime Operation CONOP document will be produced.

The purpose of the security case is to present the GNS claims in the form of a hierarchy of objectives, claims and arguments, which provides the framework in which the GNS VAI methodology has been formulated and will be implemented; and will also provide the framework in which the security regime operation CONOP will be formulated. Whilst the key requirement to be met by GNS during GDA is the identification and implementation of the VAI methodology - in order to be able to provide the basis for the production of the security regime operation CONOP and ensure continuity between GNS and the future licensee, the security case has been developed to:

- Holistically identify and articulate the physical and cyber threats to the future licensee's resources and the components of the threats; including those regulated through ONR and other statutory bodies, and other business threats;
- Holistically identify, articulate and justify the physical, digital and personnel security capabilities, and the components of the security capabilities, selected to mitigate the threats to acceptable levels i.e. the ONR security outcomes or against the future licensee's risk appetite.

The security claims stated within this security case report therefore accommodate not only for the GDA VAI and CONOP requirements but also provide the framework within which the anticipated future licensee's requirements can be accommodated.

15.2 SSER & GSR

The GSR security case sits within a wider framework of claims and arguments defined within the SSER, within which the security case claims are embedded. The direct flow-down of objectives and claims relevant to the security case from which the level 3 and 4 security case claims are derived is articulated below:

- **Fundamental Objective** -The Generic UK HPR 1000 could be constructed, operated, and decommissioned in the UK on a site bounded by the generic site envelope in a way that is safe, secure and that protects people and the environment;
- **Level 1 Claim** - PSR High Level Objective 4 Environmental Protection, Security and Conventional Safety – 'The design, and intended construction and operation, of the UK HPR 1000 will be developed to

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 37/46

reduce, so far as is reasonably practicable, the impact on the workers, the public and the environment’;

- **Level 2 Claim Security Claim 4.3** - The security threat will be managed to protect the public from the risks arising from a radiological event caused by the theft or sabotage of nuclear material or other radioactive material and supporting systems or through the compromise of sensitive nuclear information;
- **Level 3 Generic Security Claim 4.3.1** - The security regime design and operation is based on a holistic and systemic approach to the defence-in-depth security capabilities required to mitigate the threats to acceptable levels;
- **Level 3 Specific Threat Claim 4.3.2** - The security regime identifies the assumed physical and/or digital based Compromise Activities (CAs) that would need to be successfully carried out, alone or in combination, in order to achieve the identified compromise end effects including Unacceptable Radiological Consequences (URC);
- **Level 3 Specific Security Claim 4.3.3** - The security regime has the necessary security capabilities to prevent or mitigate the identified Threats from being carried out successfully including the URC based threats.

15.3 GSR Approach to Claims, Arguments and Evidence

The GSR approach to threat and security-based claims, arguments and evidence is based on the following:

- A hierarchy of level 4 claims, level 5 claims, level 6 arguments and supporting evidence;
- Claims and arguments are presented utilising a consistent format where possible;
- In general terms, each claim is formulated on a process that is applied and the output(s) achieved from the application of the process; whereas each argument is formulated based on the supporting input(s), and/or process and/or outputs;
- Each level 4 claim is assessed as being achieved when all the supporting level 5 claims are assessed as being achieved;
- Each level 5 claim is assessed as being achieved when all the supporting level 6 arguments are assessed as being achieved through the provision of the appropriate evidence;
- Where work is completed during the GDA process in order to meet ONR’s requirements and expectations, such work is or will be presented, referencing the relevant claim(s) and argument(s), and provide the evidence for the relevant argument(s) in support of the relevant claim(s);

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 38/46

- Claims are formulated to: cover the full spectrum of threats including the regulated threats and other business threats; and the security utilised to mitigate such threats;
- Claims and arguments are formulated, utilising the threat operation model and security regime operation approaches;
- Claims and arguments were appropriate will be developed during the GDA process by GNS for hand-over to the licensee, in order to ensure continuity between the two organisations and for ONR, thereby providing the golden thread during and after the GDA process;
- Claims are categorised as generic security, specific threat and specific Security.

The GSR security case is primarily broken out across three groups of claims:

- Specific Threat Claims - Specific threat claims are founded on the need to identify the physical and and/or digital Compromise Activities (CAs) that would need to be carried out in order to achieve the intended compromise end effects;
- Specific Security Claims - Specific security claims are founded on the need to ensure that the security regime operation will have the necessary security capabilities to prevent or mitigate the identified threats, where such Threats are those that are based on the compromise activities identified through the achievement of specific threat claims. This approach ensures there is direct linkage between the specific threat claims/sub-claims and the specific security claims/sub-claims;
- Generic Security Claims - Generic security claims have been formulated to ensure that:
 - The security regime operation will have the necessary security components and policies, plans and procedures, at definable levels and in place and utilised to provide the necessary security capabilities - to provide the necessary defence-in-depth security effects to maintain routine security operations and during emergency responses;
 - The security regime operation will reduce the likelihood of insiders existing; sensitive information being compromised and threat actors selecting the site as a target site or selecting targets on the site;
 - The security regime operation will have the necessary security components/capabilities to provide the necessary resilience, conservatism and sustainability; and has the necessary interoperability with external organisations;

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 39/46

- The necessary security related organisational structure and processes (including leadership and management, culture, competence management, security capability supply chain management, and Security Regime change) will be in place and utilised to maintain security integrity.

Relevant generic security claims will be utilised during the GDA process to inform the production of the security regime operation CONOP.

16. Security Regime Operation CONOP

During GDA the security regime operation CONOP, will be developed. The details of the CONOP developed in steps 3 and 4 of the GDA, accounting for UK HPR 1000 design is expected to be defined within a Tier 2 document produced in support of the GSR V1 and V2. The CONOP developed during the GDA process, is founded on the security regime operation component defined within the Security Risk Management Approach Reference [14].

GNS recognises that whilst it is the prospective licensee who will develop the site-specific security plan, it is expected that the Generic Security Report (GSR) will form the basis of this plan. The CONOP will be developed to provide the start point, enabling the detailed security regime operation design to ensure that the generic (and specific) security claims will be achieved, as defined within Security Case Report Reference [16].

16.1 Security Regime Operation CONOP

The security regime operation CONOP, which will be developed during the GDA process, is founded on the security regime operation component detailed within Security Risk Management Approach Reference [14] which could provide the start point to ensure that the detailed security regime operation design will ensure that the generic (and specific) security claims will be achieved. It is anticipated that the CONOP will be presented in terms of the security effects to be achieved displayed on an indicative site plan with examples of the security capabilities that could deliver the effects, other than those areas specific to GDA that require more detail earlier in the process such as access control.

16.2 Detail of Security Regime Operation

The detail of the security regime operation design could be based on the security regime operation CONOP and should be developed after the GDA

process by the prospective licensee. The concept of the Security Regime Operation is illustrated in Figure 2 below:

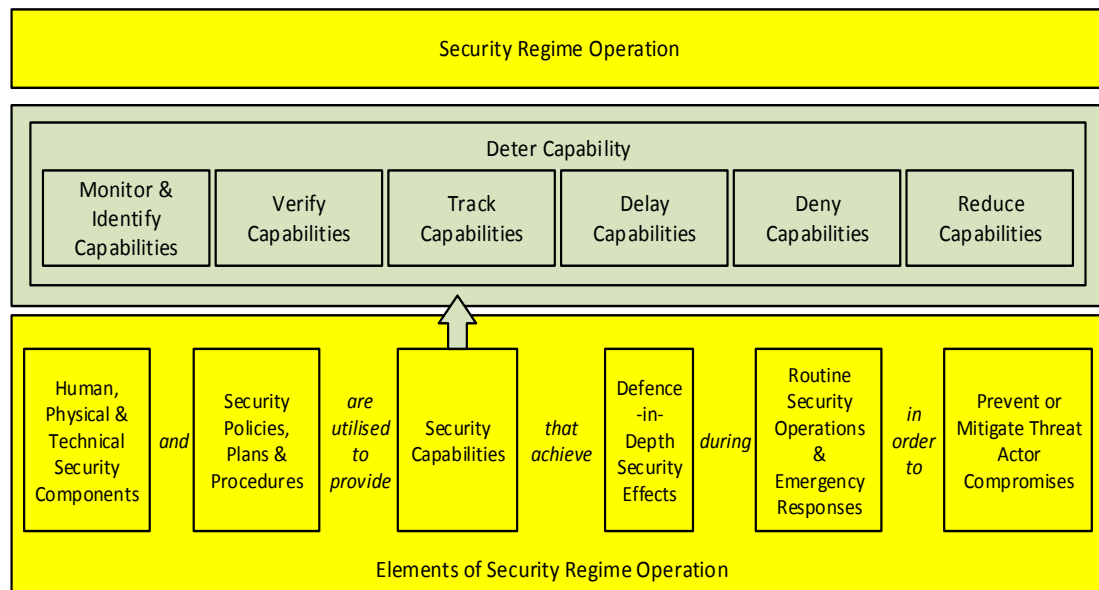


Figure 3: Concept of Security Regime Operation

The security regime operation is founded on security capabilities that are utilised to achieve defence-in-depth security effects, in order to prevent or mitigate identified threats from being carried out successfully. The security capabilities are provided through the arrangement of human, physical and/or technical security components, the utilisation of which is stated in security policies, plans and procedures. Defence-in-depth security effects are achieved through the utilisation of multiple layers of security capabilities that achieve such effects not only during potential conduct stages of threat operations but, importantly, during potential Operational Research Preparation and Planning (ORPP) stages of threat operations.

Security capabilities are required during the routine security operation to cater for the different site operating activities i.e. routine, planned and unplanned; and different threat levels and security response levels. Security capabilities are also required to be available for use during emergency responses in the form of security support and/or security responses, and during the different site operating activities and the different threat and security response levels.

Security capabilities are utilised to 'mitigate TACs from being carried out successfully'; however, in order to meet the relevant ONR security Physical Protection System (PPS) and Cyber Protection System (CPS) outcomes, security capabilities are in such cases utilised to 'prevent TACs from being carried out successfully'.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 41/46

17. Evolution of GSR V0 - V2

The GSR by nature will be a continuously developing report until the final version is submitted. The GSR will evolve throughout the GDA relative to changes in the design and safety of the UK HPR 1000. As a consequence of this evolution, it is anticipated that the design and safety case will not be complete at the end of step 3, so step 4 will involve review and revision (as required) of the GSR. It is expected that V1 will be submitted during Step 3 for assessment and entry into Step 4, the Step 3 Assessment Plan is yet to be determined, followed by V2 submission for assessment at a yet to be determined point during Step 4.

GSR V1 submission(s) will be dependent upon the assessment timescales in Step 3. However, GNS anticipate a similar approach to that of GSR V0 in that several Tier 2 documents will be submitted during Step 3 in order to enable the ONR to conduct their assessment and produce a Step 3 Assessment Report. In addition, it is expected that GSR V1 will be submitted toward the end of Step 3 for assessment during Step 4. At this juncture a similar approach may be assumed for Step 4 in terms of submissions but also periodic reviews throughout Steps 3 and 4 to ensure consistency with the reference plant, safety case and extant NIMCA. The GSR will evolve in line with GNS' GSR and the ONR assessment plans and will be delivered across steps in line with the GSR Project Plan Reference [5]. Actions that are either generated as a consequence of ONR assessment or internally identified will be captured within a Forward Action Plan that may span steps and provide an additional element of continuity between the RP and future licensee.

18. References

- [1] Safety, Security and Environment Report Delivery Strategy - HPR/GDA/REPO/0009
- [2] UK HPR1000 GSR Delivery Strategy - HPR/GDA/REPO/0012
- [3] Nuclear Industries Malicious Capabilities (Planning) Assumptions – 2015 Review, October 2015
- [4] GNS Scope for UK HPR1000 GDA Project - HPR/GDA/REPO/0007
- [5] GNS GSR Project Plan - GDA/REC/GNS/002679

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 42/46

[6] ONR, Security Assessment Principles for the Civil Nuclear Industry, 2017 Edition, Version 0, March 2017

[7] GNS Plant Design & Information Report – HPR/GDA/REPO/0060

[8] UK HPR1000 Design Control Strategy - HPR/GDA/REPO/0006

[9] GNS Requirements on Optioneering and Decision Making - HPR/GDA/PROC/0012

[10] UK HPR1000 Modification Control Procedure - HPR/GDA/PROC/0053

[11] Technical Committee Operation Guidance - HPR/GDA/PROC/0024

[12] UK HPR1000 Cross Cutting Forum Terms of Reference – GDA/REC/GNS/001692

[13] ONR, National Objectives, Requirements and Model Standards, Version 2, April 2014

[14] GNS Security Risk Management Approach - HPR/GDA/PROC/0060

[15] GNS Vital Area Identification Methodology - HPR/GDA/PROC/0062

[16] GNS Security Case Report - HPR/GDA/PROC/0064

[17] ONR, Nuclear Safety Technical Assessment Guide, Target Identification for Sabotage, CNS-TAST-GD-6.2, Rev. 0, March 2017

[18] GDA Schedule Plan – HPR/GDA/REPO/0014

Appendix 10A Terminology and Definitions

T-10A–1 Security Definitions

Word/Phrase	Definition
Availability (Information)	For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
Candidate Critical SSC	A potential target which forms part of a Potential Compromise Activity.
Computer Based Systems Important to Safety (CBSIS)	A safety system or safety related system performing category A, B or C safety functions whose correct functioning relies on the use of one or more microprocessors and/or one or more Programmable Complex Electronic Components (PCEC). The definitions of category A, B and C safety functions are taken to mean those specified in ONR's Safety Assessment Principles for Nuclear Facilities 2014 edition, Revision 0.
Compromise Activity/Activities	Compromise Activity is the activity that needs to be carried out by a threat actor (or actors) in order to achieve a compromise end effect; and compromise activities are a group of activities that need to be carried out by a threat actor (or actors) in order to achieve a compromise end effect.
Compromise End Effect	Compromise end effect is the end effect that a threat actor (or actors) intends to achieve as a result of carrying out a compromise activity or multiple compromise activities.
Compromise Method	Compromise method is the method carried out by a threat actor (or actors) against a compromise method target in order to achieve a compromise effect which may be the compromise end effect.
Confidentiality (Information)	Is the property, that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Cyber	Computers or computing processes i.e. Information Technology or Operational Technology.
Defence-In-Depth Security Effects	Defence-in-depth security effects are the effects achieved, through the utilisation of multiple layers of security capabilities, against potential threat operation activities including during the ORPP stage and conduct stage.
Digital	The transmittal or storage of information through digital signals.

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 44/46

Word/Phrase	Definition
Information Technology	Information Technology is the use of computers to store, retrieve, transmit and manipulate data or information.
Integrity (Information)	In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner.
Nuclear Material	Plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; <i>uranium enriched in the isotope 235 or 233</i> ; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore residue; any material containing one or more of the foregoing.
Operational Technology	Operational Technology refers to the hardware and software used on the plant network.
Passive safety	The provision and maintenance of a safety function without the need for an external input such as actuation, mechanical movement, supply of power or operator intervention.
People	People are site people and/or the public.
Radioactive Material	Radioactive material, as defined in CPPNM; radioactive sources, as defined in Code of Conduct for Safety and security of Radioactive Sources and other radioactive substances containing nuclides which undergo spontaneous disintegration (a process accompanied by the emission of one or more types of ionizing radiation, such as alpha and beta particles, neutrons and gamma rays.
Radioactive Source	Radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It also means any radioactive material released if a radioactive source is leaking or broken, but does not mean material encapsulated for dispersal, or nuclear material within the nuclear fuel cycles of research and power reactors.
Resilience (Security)	[Security] resilience is the spare capacity that exists within each suite of security capabilities to ensure, that when a security capability becomes unavailable, an alternate capability can be utilised to provide the necessary security effect within the acceptable time period.
Resilience (Safety)	Safety resilience is the resilience provided through the plant system design including redundancy, diversity and segregation.

Word/Phrase	Definition
Sabotage	Sabotage is any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.
Safety function	A specific purpose that must be accomplished for safety.
Security Capabilities	Security capabilities are the capabilities provided through the integrated use of security components, to deliver security effects.
Security Components	Security components are the human, physical and technical components that are utilised to provide security capabilities.
Security Effects	Security effects are the effects that are provide by security capabilities used to mitigate threat operations from being carried out successfully.
Security Integrity	Security integrity is the completeness of the security in terms of the licensee.
[ONR] Security Outcomes	ONR security outcomes are the physical protection system and cyber protection system outcomes, responses and required effects that the licensee should seek to achieve.
Security Regime	Security regime is the sum of all the security components and security policies, plans and procedures that provide the security capabilities; noting that some components are not physically located at the licensee site.
Security Regime Operation	Security regime operation is the utilisation of security capabilities to ensure that the threat operations that may be mounted against the licensee are mitigated from being carried out successfully to acceptable levels.
Security Vulnerability Assessment	Security Vulnerability Assessment is the process used to display that a Security Regime Operation (or parts thereof) prevent, or mitigate to acceptable levels, a specific threat operation (or a group of threat operations) from being carried out successfully; or where this is not the case, the assessment identifies any vulnerabilities.
Sensitive Nuclear Information	Sensitive Nuclear Information (SNI) is information that if compromised could contribute to the planning, preparation and conduct of a successful threat operation resulting in either the theft of NM/ORM or URCs through sabotage.
Structure System or Component	A general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human

UK HPR1000 GDA	Generic Security Report	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 46/46

Word/Phrase	Definition
	factors. Structures are the passive elements: buildings, vessels, shielding, etc. A system comprises several components, assembled in such a way as to perform a specific (active) function. A component is a discrete element of a system.
Threat Actor	Threat actor is a threat person who carries out the compromise activity/activities; and threat actors are a group of persons that fit the same criteria.
Threat Actor Compromise	Threat Actor Compromise is the sum of the compromise activity/activities and the compromise end effect achieved as a result of carrying out a compromise activity/activities successfully.
Threat Assumption	Threat assumption is an informed supposition based on intelligence, operational experience and judgement that is formulated in the absence of fact, about potential threat operations or components of such operations.
Unacceptable Radiological Consequences	Unacceptable Radiological Consequences are defined as an effective dose (including committed effective dose) over 24 hours at the facility, to the most limiting member of the public, assuming a ground level release.
Vital Area	Vital Area is an area containing NM/ORM (including radioactive sources), or equipment, systems, structures or devices, the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant DBT, could directly or indirectly result in URCs, thereby endangering public health and safety by exposure to radiation.