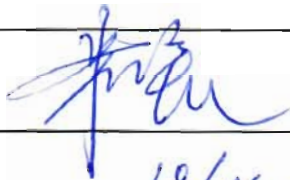



Revision	Approved by	Number of Pages
000		25
Approval Date	10/11-17	
 <b>General Nuclear System Ltd.</b>		
UK HPR1000 GDA Project		
<b>Document Reference:</b>	<b>HPR/GDA/PSR/0027</b>	
<b>Preliminary Safety Report</b> <b>Chapter 27</b> <b>Security</b>		
<p>This document has been prepared on behalf of 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 type="checkbox"/>
GNS all staff	<input type="checkbox"/>
GNS and BRB all staff	<input checked="" type="checkbox"/>
CGN	<input checked="" type="checkbox"/>
EDF	<input checked="" type="checkbox"/>
Regulators	<input checked="" type="checkbox"/>
Public	<input checked="" type="checkbox"/>

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 3 / 25

## Table of Contents

27.1	List of Abbreviations and Acronyms .....	4
27.2	Introduction.....	6
27.3	Regulatory Security Assessment for the HPR1000 .....	6
27.4	UK Security Requirements .....	12
27.5	Methodology for the Identification of Vital Areas.....	21
27.6	CGN Security Design & Technical Team .....	22
27.7	Conclusion.....	23
27.8	References .....	24

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 4 / 25

## 27.1 List of Abbreviations and Acronyms

CDF	Core Damage Frequency
CISO	Chief Information Security Officer
CNS	Civil Nuclear Security
DBT	Design Basis Threat
DCS	Digital Control System
DSO	Departmental Security Officer
FCG Unit 3	Fangchenggang Nuclear Power Plant Unit 3
GDA	Generic Design Assessment
GNS	General Nuclear System Limited
GSR	Generic Security Report
HMG	Her Majesty's Government
HPR1000	Hua-long Pressurized Reactor
HPR1000 (FCG3)	Hua-long Pressurized Reactor under construction at Fangchenggang nuclear power plant unit 3
IAOs	Information Asset Owners
I&C	Instrumentation and Control
IPS	Integrated Protection Solution
IT	Information Technology
MRF	Mass Release Frequency
NIMCA	Nuclear Industries Malicious Capabilities (Planning) Assumptions
NNSA	National Nuclear Safety Administration
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
PCER	Pre-Construction Environment Report
PCSR	Pre-Construction Safety Report
PSA	Probabilistic Safety Assessment
PSAR	Preliminary Safety Analysis Report

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 5 / 25

PSR	Preliminary Safety Report
SIRO	Senior Information Risk Owner
SNI	Sensitive Nuclear Information
SyAPs	Security Assessment Principles
TAG	Technical Assessment Guide
T <sub>1/2</sub>	Half life
UK HPR1000	The UK Version of the Hua-long Pressurized Reactor
URC	Unacceptable Radiological Consequence
VAI	Vital Area Identification

UK HPR1000 GDA	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 6 / 25

## 27.2 Introduction

This chapter will discuss, at a principle level, the process of review for the Hua-long Pressurized Reactor (HPR1000) to satisfy the National Nuclear Safety Administration (NNSA) and UK Government requirements for internal processes and arrangements that General Nuclear System Limited (GNS) will be putting in place or are progressing to support delivery of the GDA UK HPR1000 Project. A separate submission covering the Generic Security Report (GSR) will be developed during the course of the Generic Design Assessment (GDA) for delivery in parallel with the Pre-Construction Safety Report (PCSR) and Pre-Construction Environment Report (PCER). This document will describe the arrangements to support the secure operation of the UK version of the Hua-long Pressurized Reactor (UK HPR1000) and therefore support the regulator's in depth security review.

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. Sensitive Nuclear Information (SNI) need 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 SNI and other classified material. Discussions have been made during the preparation of this document to exchange security marking information protocols for the UK, China and France to establish the types of information that will be exchanged, developed and stored during this early phase of the project. Processes have either been put in place or are under development to both identify and control SNI for the UK HPR1000 project.

However, information on the topic of Security is itself sensitive and subject to such controls. Consideration of the approach to information related to security classified topics in the UK needs access to information that is restricted to UK nationals only on a need to know basis. These are not included in the Preliminary Safety Report (PSR) and will be provided in a separate document to the relevant authorities developed by the UK Security team within GNS.

Effective security arrangements in the nuclear industry are essential to prevent the theft of nuclear or other radioactive materials, the sabotage of nuclear facilities and to protect SNI. Therefore, ONR produces a series of documents, which contains security policy framework, security culture, sensitive information and other items, to assist ONR inspectors in their assessment, Reference [1] and [2].

## 27.3 Regulatory Security Assessment for the HPR1000

The following is a brief overview of the assessment performed by NNSA to support the construction and licensing of the HPR1000 in China.

Nuclear power plant security arrangements are mainly intended to prevent the destruction of important nuclear power plant equipment and nuclear material theft or illegal transfer,

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 7 / 25

so as to avoid unacceptable radioactive consequences. In order to ensure the safety of nuclear power plants and nuclear materials, and in accordance with the requirements of nuclear safety regulation HAD501-02, Reference [3], a nuclear power plant must establish a security arrangement and must implement the highest level of physical protection. The security arrangement is mainly intended to protect important equipment on nuclear facilities and nuclear materials, but is also there to detect, monitor, alarm and mitigate the intrusion of malware. It can also be used to prevent the nuclear facilities against threats, destruction and criminal activities, and to prevent critical equipment from damage. In addition, the security arrangements reduce the risk of loss of nuclear materials by providing a safe and reliable operating environment for nuclear facilities.

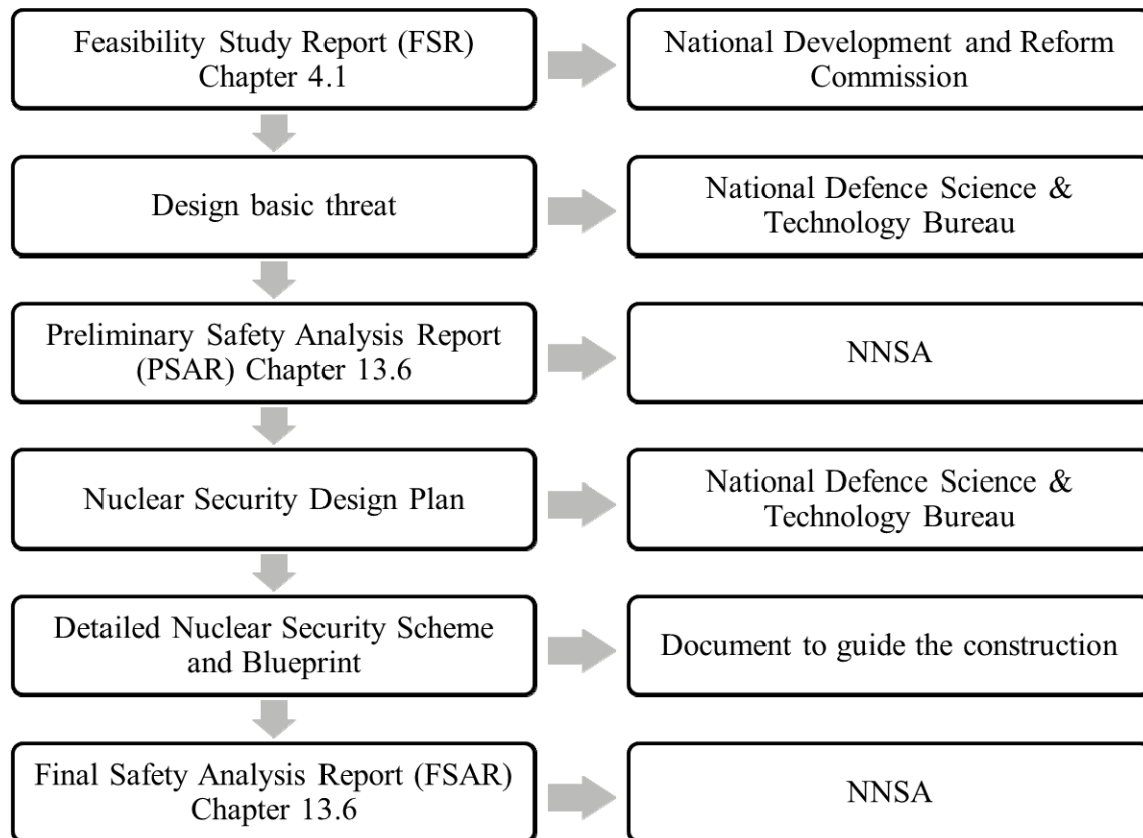
Fangchenggang Nuclear Power Plant Unit 3 (FCG Unit 3) has implemented the top-level protection in term of the security arrangement. According to the different degrees of importance of the various facilities of the nuclear power plant, the plant is divided into three different areas, control area, protection zone and vital area. The security level of each security area gradually strengthened and each protection area has a perimeter barrier wire fence to form a complete closed perimeter. It combines personnel protection and equipment protection: For personnel protection, it organizes the implementation of system and responsive force, for equipment protection, it provides effective detection and mitigation. At the same time, in order to effectively prevent hacker attacks, anti-intrusion detection system and anti-virus software will be installed in the computer system of FCG units 3 and 4, as well as the system being completely physically isolated from the outside, without any physical interface.

As one of the key area for the assessment of the NNSA, the security arrangement for FCG Unit 3 has been addressed in the Preliminary Safety Analysis Report (PSAR) chapter 13.6, and it has been reviewed and approved by the NNSA. The key topic areas covered in the review include detection, delay, response, and cyber protection. No issues were raised by the regulator.

PSAR chapter 13.6 includes basis of design, organization, responsibility and division of labor, principal of design, physical protection zoning and physical barrier, defending force, introduction of subsystem such as access control system, video monitoring system and intrusion detection and alarm system, emergency handling, etc.

In addition, for HPR1000 (FCG3), a separate physical protection arrangement is compiled and reviewed by the National Defence Science & Technology Bureau. After the approval of security arrangements detailed design work and construction design work is carried out. When the construction reaches a certain stage, the Final Safety Analysis Report (FSAR) chapter 13.6 is compiled and sent to the NNSA as the Final Safety Analysis Report and as the supporting document in the application for the fuel feeding and fuel loading permits, Reference [4].

The following is the process for Security Plan Development in China:



F-27.3-1 The Process For Security Plan Development Chart

The following are details of Chinese security regulation that the HPR1000 must meet at FCG Unit 3:

The threat factors that the nuclear facilities may be subject to shall be analyzed and classified, in order to sort out the Design Basis Threat (DBT). The possible threat factors include the type of criminals, their motive, scale, capacity and the possible methods and strategies. The potential criminals include internal, external and the collusion of both inside and outside personnel. Only when the DBT of the nuclear facilities is reviewed and approved by the relevant national authority can it be used as the basis for designing physical protection systems.

### **Graded and Zoned Protection**

Security grading is graduated from high to low with Grade 1 being high and Grade 3 low. In addition, security zoning is broken down by: vital area, protected area and access control area. Using this graded and zoned approach the appropriate security systems are implemented for the physical protection of the nuclear facilities according to the importance of the protection target and its potential risk class.

HPR1000 generic approach to security zoning is a 3 zoned approach: external/outside zone / internal – protected zone / vital zone. Each zone's security posture increases as you work inwards from the extremity of the site.



<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 9 / 25

For HPR1000, nuclear security includes all buildings and system devices in the control area. Buildings related to administration and office work are located in the control area. Buildings related to production are located in the protected area. Buildings related to nuclear safety such as nuclear island are located in the vital area. All the buildings and system devices above are included in the nuclear security of HPR1000.

### **Complete, Reliable and Effective System**

The physical protection system considers several factors. The coordination between detection, delay and response shall be ensured, the functions of the physical protection devices shall be a complete and effective combination of response force, meanwhile the technical protection measures shall be achieved. Therefore, a complete, reliable and effective Physical protection system shall be built.

### **Defence in Depth and Balanced Protection**

The physical protection system shall be equipped with multiple physical barriers according to the facility's class, and configured with multiple layers of detection and alarm systems using different technology. Different parts in the same protected area shall have the same safety protection level and there shall not be any obvious vulnerabilities. Defence in depth and balanced protection for nuclear facilities is to be achieved.

### **I&C Cyber Security**

The design of the UK HPR1000 (FCG3) takes into account the design requirements of cyber security and that of the Digital Control System (DCS). The supplier must meet the requirements of Chinese national regulations and reference the relevant requirements of RG 1.152, Reference [5], considering how to realize those requirements in order to reduce risks from cyber-attacks or other adverse computer challenges.

The cyber security design of the I&C systems of HPR1000 (FCG3) is in accordance with Chinese regulations, Reference [6], [7], and so on.

According to the requirements of Chinese regulations, information systems are divided into five levels based on the importance to national security, economic development and social life, from low to high. The DCS is graded as level 3. The damage of level 3 information system could cause serious damage to social order and public interest, or damage to national security.

The cyber security requirements are divided into management and technology requirements according to the specific implementation methods. The management and technology requirements are comprehensively used in the guidance for cyber security design for level 3.

Management requirements include the safety management institution, safety management organization, personnel safety management, system building management and system operation management.

Technology requirements cover the aspects of physical security, network security, host security, application security and data security.

Cyber security of I&C systems adopts the technical and management measures in order to achieve the security aim which is to enhance cyber security management on I&C systems, to prevent cyber attacking and aggrieving on I&C systems from hacker and vicious code etc., and ensure I&C systems safety and stabilized operation. Cyber security considers in the lifetime of the I&C system.

### Nuclear Material Protection

The nuclear materials are classified into three physical protection grades according to the damage degree of the type, quantity, degree of enrichment, radiation level, physical and chemical state of the nuclear materials. There are three types of nuclear materials in nuclear power plants, namely new fuel, spent fuel and radioactive waste. The higher the level of protection, the tighter the corresponding nuclear security measures, and the lower the likelihood of theft and destruction.

The new fuel and spent fuel protection is divided into three levels of protection in accordance with the quality of nuclear material, its volume and potential degree of harm associated.

T-27.3-1 Categorization of the New Fuel and Spent Fuel

Material	Form	Category I	Category II	Category III
Plutonium	Unirradiated	2 kg or more	10 g to 2 kg	Less than 10 g
Uranium	Unirradiated, Uranium enriched to 20% or more	5 kg or more	1 kg to 5 kg	10 g to 1 kg
	Unirradiated, Uranium enriched to 10% but less than 20%		20 kg or more	1 kg to 20 kg
	Unirradiated, Uranium enriched to less than 10% (not including natural uranium or depleted uranium)		300 kg or more	10 kg to 300 kg

Material	Form	Category I	Category II	Category III
Tritium	Unirradiated	10 g or more	1 g to 10 g	0.1 g to 1 g
Lithium	Enriched lithium		20 kg or more	1 kg to 20 kg

Note: 1. Plutonium and uranium are categorized by the amount of element but not by the mass effective

2. Tritium and material and products that contain tritium are categorized by the amount of tritium

3. Enriched lithium and material and products that contain enriched lithium are categorized by the amount of lithium (Enriched lithium refers to a larger concentration of isotopic lithium-6 than natural lithium)

According to the physical form of radioactive Waste, it is divided into three categories, respectively air-borne waste, liquid waste and solid waste. According to the radioactive concentration and specific radioactivity, it is divided into low-activity levels, medium-activity levels and high-activity levels. Each level therefore corresponds with an appropriate level of physical protection.

Classification System of Radioactive Waste is as followed tables.

#### T-27.3-2 Classification of Radioactive Waste Management

Type	Class	Name	Radioactive Concentration Av
Air-borne Waste	I	Low-activity	Emission Limit $<Av < 4 \times 10^7$ (Av, Bq/m <sup>3</sup> )
	II	Medium-activity	$4 \times 10^7 < Av$ (Av, Bq/m <sup>3</sup> )
Liquid Waste	I	Low-activity	Emission Limit $<Av < 4 \times 10^6$ (Av, Bq/l)
	II	Medium-activity	$4 \times 10^6 < Av < 4 \times 10^{10}$ (Av, Bq/l)
	III	High-activity	$4 \times 10^{10} < Av$ (Av, Bq/l)

T-27.3-3 Specific Radioactivity Am, Bq/Kg

		$T_{1/2} \leq 60d^{(1)}$	$60d < T_{1/2} \leq 5a^{(2)}$	$5a < T_{1/2} \leq 30a^{(3)}$	$30a < T_{1/2}$	$\alpha$ Waste
Solid Waste	I Low-activity	Clearance Level $< Am < 4 \times 10^6$	Clearance Level $< Am < 4 \times 10^6$	Clearance Level $< Am < 4 \times 10^6$	Clearance Level $< Am < 4 \times 10^6$	The Am of the long-life radioactive nuclides in a single package is higher than $4 \times 10^6$ ; the average Am of each package is higher than $4 \times 10^5$ .
	II Medium-activity	$4 \times 10^6 < Am$	$4 \times 10^6 < Am$	$4 \times 10^6 < Am < 4 \times 10^{11}$	$4 \times 10^6 < Am^{(4)} < 4 \times 10^{10}$	
	III High-activity			$4 \times 10^{11} < Am^{(5)}$	$4 \times 10^{10} < Am^{(6)}$	

Note:

- (1) including radioactive nuclide iodine—125( $T_{1/2}=60.12d$ )
- (2) including radioactive nuclide cobalt—60( $T_{1/2}=5.271a$ )
- (3) including radioactive nuclide caesium—137( $T_{1/2}=30.17a$ )
- (4) and the heat release rate is less than or equal to  $2kw/m^2$
- (5) or the heat release rate is higher than  $2kg/m^2$
- (6) and the heat release rate higher than  $2kw/m^2$

### Simultaneous Design, Construction & Operation

The physical protection system shall be designed, constructed and put into operation simultaneously with the main works of the nuclear facilities.

### 27.4 UK Security Requirements

Following a review of the information available in the public domain on the security requirements in the UK, below is a summary which GNS is considering in the set-up of the organization and day to day operation.

There must be an approved security plan for each nuclear premise. A security plan must describe in writing the standards, procedures and arrangements adopted or to be adopted by the responsible person to ensure the security of:

- The nuclear premises,

UK HPR1000 GDA	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 13 / 25

- Any Category I/II nuclear material and Category III nuclear material used or stored on the premises,
- Any equipment (or software) used or stored on the premises in connection with activities involving nuclear material,
- Any SNI.

UK security regulation is based upon the NISR 2003 (as amended), Reference [8], which stipulates there must be an approved security plan in place for nuclear premises, combined with the newly released ONR Security Assessment Principles (SyAPs), April 2017, and the UK DBT the NIMCA provide the key baseline UK regulatory documentation for the production of the GSR. It is worth noting that the SyAPs are a significant change in regulatory approach by ONR (CNS) in that these are effects/outcome focused where their predecessor NORMS was a more prescriptive approach to security regulation. This is a key differing point to draw upon in that Chinese security regulation remains of the prescriptive nature and thus the transition to SyAPs and understanding this approach will be a new challenge. The UK HPR1000 will be the first GDA and GSR to be assessed against the SyAPs. An appropriate security governance structure should consist of a Senior Information Risk Owner (SIRO), a Departmental Security Officer (DSO) who can manage day-to-day protective security, a Chief Information Security Officer (CISO), and Information Asset Owners (IAOs) across the distinct business units. Further to this the information risk assessment and risk management specialists, other specialists relevant and specific to the organization's needs.

To cultivate a strong security culture, the organization must have a security culture that supports business and security priorities and is aligned with HMG's overarching priorities and the organization's own appreciation of risk. Training which encourages personal responsibility and good security behaviours will be an essential element to support how GNS will run on a day to day basis. Robust processes and systems to deliver work, coupled with the mechanisms to drive continuous improvement, tackle poor and inappropriate behaviour, enforce sanctions and encourage the sharing of best practice will be essential to the success of GNS.

For information security, the staff must be well trained to exercise good judgment, take responsibility and be accountable for the information they handle, including all partner information. Mechanisms and processes will be put in place to ensure assets are properly classified and appropriately protected. Confidence will be provided to the regulator that security controls are effective and that systems and services can protect the information they carry.

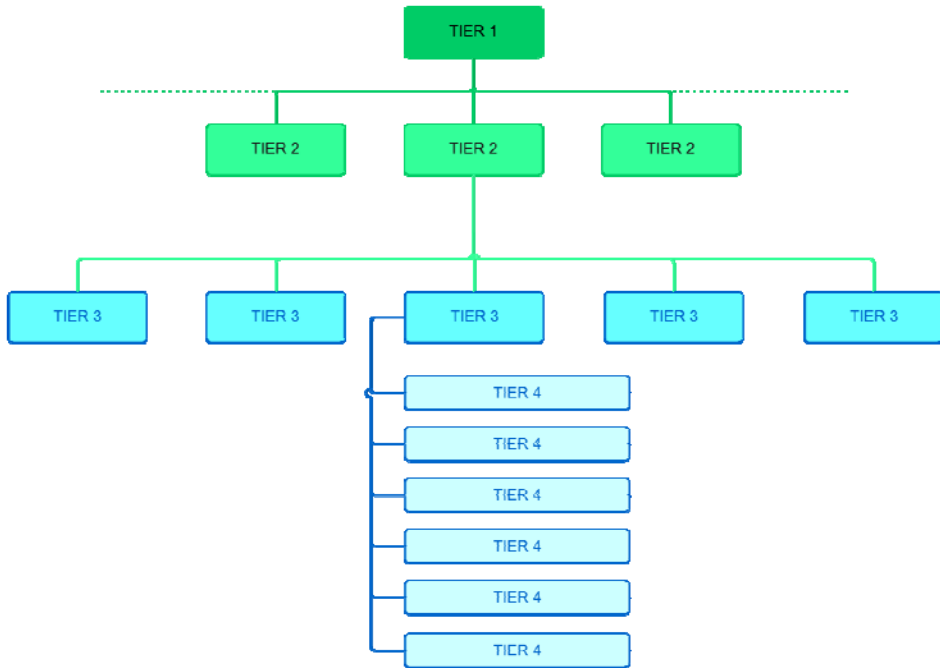
For the GDA process, the Office for Nuclear Regulation (Civil Nuclear Security) will assess the GDA submission for UK HPR100, the GSR, through Steps 2 to 4. Step 1 is the initial step to establish the HPR100 security process and regulation as well as establishing UK Regulation 22 compliance as a business. Step 1 includes the production of

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 14 / 25

submissions for Step 2 entry, namely the PSR Chapter 27 and Regulation 22 compliance enabling documentation. As the GSR progresses from Step 2 onwards such information as the generic plant layout, design information relating to the fabric of buildings, process descriptions of the technology, philosophy for plant control, other Information Technology (IT) systems ,management of SNI and physical layouts for control systems, emergency back-up safety system descriptions and personnel security policies and procedures, the findings of any analysis done to look into the impact of major site events, Information Security policies and procedures, visitor management standards, Security Governance etc. will be provided.

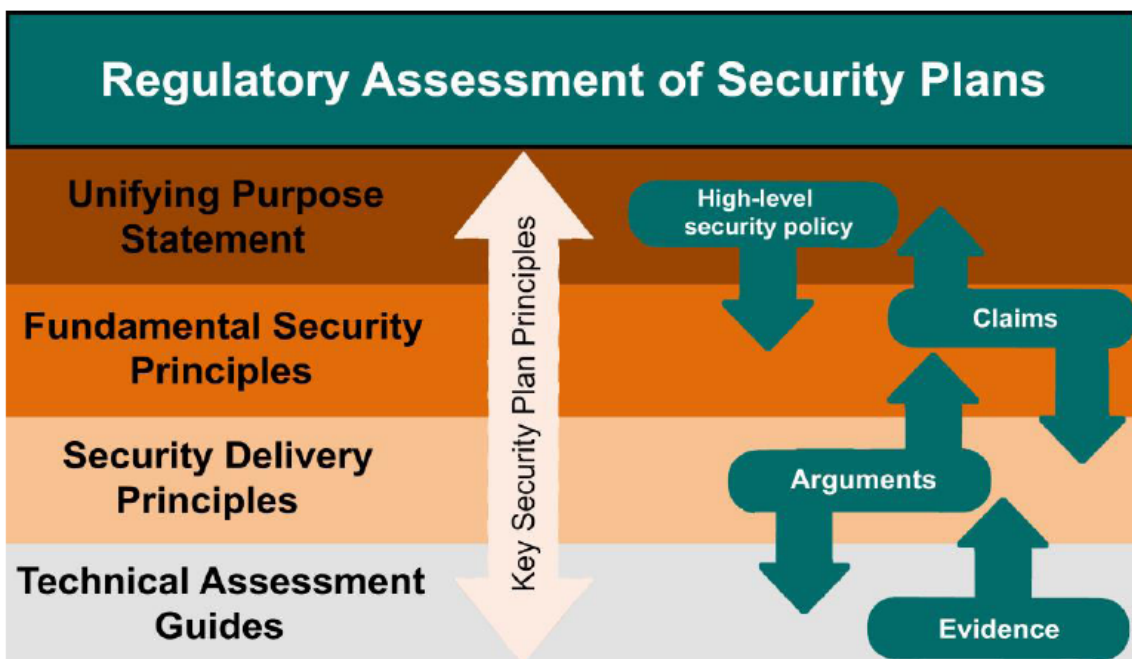
Step 2 onwards will analyse, identify and articulate the vulnerabilities and security mitigations required for the UK HPR1000 in light of both the DBT and best practice. The ONR must be able to provide assurance to Her Majesty’s Government that the state of security within the civil nuclear industry is in line with their expectations. This is achieved through the publication of the Chief Nuclear Inspector’s Annual Assurance Report, which provides an overview of the safety and security of the UK nuclear, regulated estate. It presents data relating to regulatory activity, events and issues, together with a supporting narrative. It also provides evidence and an explanation that supports the safety and security judgments attributed to the regulated sites. The overall regulatory priority for security considers the combined performance in three themes: Security Delivery, Security Plans & Capabilities and Security Leadership & Culture. The first two themes cover the lagging indicators, which are reactive measures of success or failure. It is here that the majority of quantitative data is available for analysis. Leadership and culture contains leading indicators, which are forward looking and strategic in nature. They are of great importance due to their influence on performance, however, data in this theme tends to be binary or qualitative, requiring a greater degree of inspector opinion and judgment, Reference [9].

### **UK Security Regulatory Requirements**



F-27.4-1 the Security Assessment Principles Structure Chart

Tier 1 includes a unifying purpose statement and introduction, Tier 2 includes ten fundamental security principles (FSyPs), Tier 3 includes security delivery principles (SyDPs), Tier 4 includes technical guidance (suite of Technical Assessment Guides (TAGs) and reference material aligned to SyDPs). The security assessment principles structure includes key security plan principles, Reference [10].

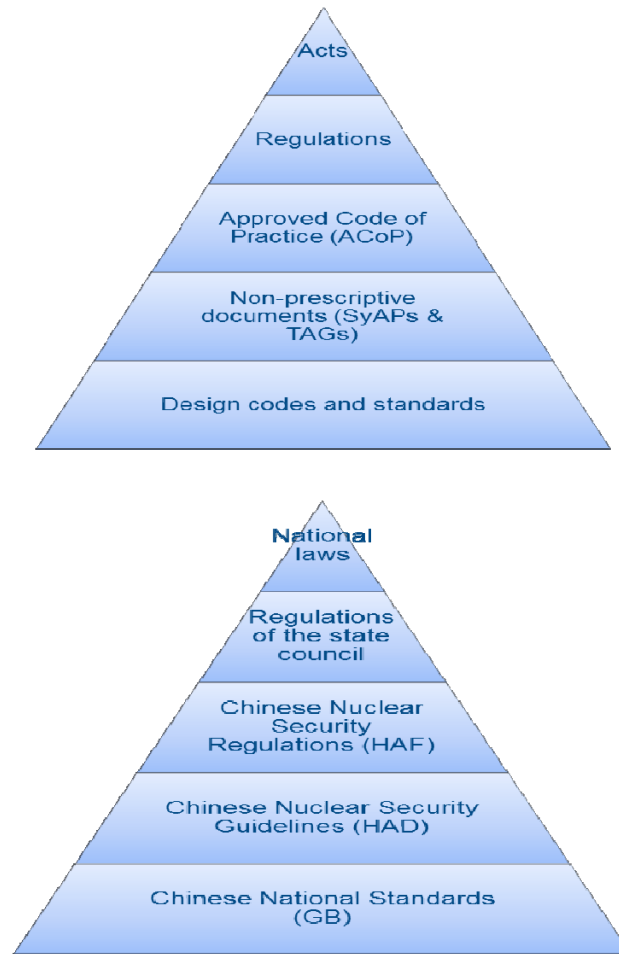


F-27.4-2 the Regulatory Assessment of Security Plans

T-27.4-1 Chinese Nuclear Security Guidelines

Section	Title	Content
1	Introduction	Purpose
		Scope
2	Basic Principles	Design Basis Threat
		Graded and Zoned Protection
		Complete, Reliable and Effective System
		Defense in Depth and Balanced Protection
		Simultaneous Design, Construction and Operation
3	Organizational Structure and Responsibilities	Organizational Structure
		Duties
4	Grading and Zoning	Grading of Physical Protection for Nuclear Facilities
		Zoned Protection of Nuclear Facilities
5	Physical Protection for Permanent Establishment	Guard and Ward
		Physical Barrier
		Entrance and Exit Control
		Technical Protection Measures
		Security Control Center or Guard Room
		Emergency Handling
6	Cyber Security and Information Assurance	Classified Protection of Information Security
		Safety Protection of Power Monitoring System
		Power Network and Information Security





F-27.4-3 Comparison of Security Regulatory Structure

For the comparison above it is clear that Chinese and United Kingdom legislation and regulation processes differ however, there is a similar approach to regulation. In addition, UK security guidelines and policy like Chinese regulation often use or refer to IAEA standards as a baseline.

The United Kingdom's reference to the IAEA, IEC and IEEE on the basis of its domestic legal system is more direct, some guidelines are even complementary to these international norms and the UK's assessment process for nuclear power plants, and in addition to providing the proper documentation, also proves that the method used in the document is well practiced. The method of evaluation is target driven and result based.

### Comparison of Security Regulation

The UK's nuclear security-related regulations include the Energy Act 2004 and Nuclear Industry Security Regulation 2003 (NISR as amended). The NISR is the main law in the UK on nuclear security, and its direct upper act is the anti-Terrorism Crime and Security Act 2001 (Anti-Terrorism, Crime and Secure Act). On the basis of NISR, and the Nuclear Industries Malicious Capabilities (Planning) Assumptions (NIMCA) which is the UK Design Basis Threat (DBT) provide guidance and a baseline threat to which the UK civil nuclear industry works to in order to fulfil its security obligations. The last and most

UK HPR1000 GDA	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 18 / 25

extensive level is the guideline and the national requirement. China's physical protection laws and regulations system is divided into five levels: national law, the State Council regulations, the State Council ministries and departments of regulations, guidelines and standards. The national law is the top-level document, is the legal basis to carry out the physical protection work, the content is strong and principled, but the content is relatively simple; in administration, the State Council approves the issue of the State Council's regulations as the administrative regulations of the State Council, which is the refinement of the state law in a certain aspect, and stipulates the legal requirements in this respect. Then, The national administrative authorities will, in the framework of national laws, according to the corresponding provisions in the national law, combined with the management characteristics of their respective departments, the establishment of relatively detailed departmental rules and regulations to ensure the day-to-day management of the development; Finally, the national administrative authorities must also develop a large number of guidelines and standards that are detailed to the operational level, In order to standardize and standardize the work of physical protection.

By analysing the specific content of the legislation, we find that there are many similarities between the two countries, the following are the four aspects we choose to explain.

### **Example 1:**

#### SyAPs - UKKSYP2 - THE THREAT

Protection systems should be designed, evaluated and tested using the state's Design Basis Threat.

It is essential that a DBT is used as the basis for the design, evaluation and testing of protection systems to seek assurance that it will meet a defined security outcome. Within the UK, the DBT malicious capabilities assessed as confronting the civil nuclear industry and assumptions about the composition and capabilities of terrorist groups and others posing a threat are described in detail in the current NIMCA document, issued by BEIS. The NIMCA, which incorporates assessment provided by the relevant government authority, is updated and amended in line with IAEA recommendations.

#### HAD501/02 - China

##### 2.1 Design Basis Threat

The threat factors that the nuclear facilities may be subject to shall be analyzed and classified, in order to sort out the design basis threat. The possible threat factors include the type of criminals, their motive, scale, capacity and the possible methods and strategies. The potential criminals include internal criminal, external criminal and collusion of the inside and outside. Only when the design basis threat of the nuclear facilities is reviewed and approved by the relevant national authority can it be used as the basis for designing physical protections system.

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 19 / 25

**Example 2:**

SyAPs - UK

FSYP 6 - Physical Protection Systems

SyDP 6.4 - Vulnerability Assessments

Duty holders should satisfy themselves that their physical protection system achieves the required security outcome through undertaking vulnerability assessments.

HAD501/02 - China

2.4 Defence in Depth and Balanced Protection

The physical protection system shall be equipped with multiple physical barriers according to the facility class, and configured with multiple layers of detection and alarm systems of different technologies. Different parts in the same protected area shall have basically the same safety protection level, and there shall not be any obvious weak points and hidden trouble. Defence in depth and balanced protection for nuclear facilities shall be achieved.

**Example 3:**

SyAPs - UK

FSYP 9 - POLICING AND GUARDING

Duty holders must demonstrate effective guarding and policing arrangements, integrating the operations of relevant police forces (e.g. CNC, BTP) and security guard services.

SyDP 9.1 - CNC Response Force

Duty holders should facilitate CNC deployment that is appropriate to achieve the required security outcome.

SyDP 9.2 – Local Police Operations in Support of the Duty holder

Duty holders should facilitate local police forces' provision of support by way of assistance to the CNC or delivering a response to the site in respect of terrorist, criminal or protest activity.

SyDP 9.3 – Security Guard Services

Duty holders should employ civilian security guards to provide the unarmed guarding that conducts nuclear security operations as described in the site security plan such as patrolling, access control and searching; and, who deliver or enable the immediate response to a security event.

HAD501/02 - China

5.1 Guard and Ward

UK HPR1000 GDA	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 20 / 25

Corresponding guard force shall be deployed according to the physical protection grade of the nuclear facilities. They shall include armed police, guards and security workers, pass strict training and evaluation, and are equipped with necessary outfit and communication tools. Duties for the guard force:

To carry out guard, watch and twenty-four-hour patrol tasks at the entrance and exit of the physical protection area, critical parts and inside the boundary;

To strictly control the access to the nuclear material storage site, important nuclear equipment warehouse and other critical parts, and carry out corresponding examination and registration works;

To carry out review and verification at the site where alarm is generated;

To carry out emergency tasks when emergency occurs; it mainly includes: to report timely to the supervisor and relevant authorities; to quickly block, track and arrest the invaders, to evacuate and rescue the public immediately.

#### **Example 4:**

SyAPs - UK

#### FSYP 10 - EMERGENCY PREPAREDNESS AND RESPONSE

Duty holders must implement and maintain effective security emergency preparedness and response arrangements which are integrated with the wider safety arrangements.

##### SyDP 10.1

Duty holders should have in place incremental counter terrorism measures that can be implemented in response to changes in threat; and EP&R arrangements to deal with any nuclear security event arising and the potential effects.

##### SyDP 10.2

Duty holders should implement a regime of exercising to train personnel and test the efficacy of the nuclear security contingency plans.

##### SyDP 10.3

Duty holders should implement structures and processes to ensure effective command, control and communications arrangements during and post nuclear security events.

HAD501/02 - China

#### 5.6 Emergency Handling

##### 5.6.2 Emergency Handling Scheme

Detailed emergency handling scheme shall be developed and strictly implemented for the nuclear facilities. The basic contents of the scheme include: preventing the man-made damage to the nuclear facilities; preventing the theft or illegal transfer of the nuclear

UK HPR1000 GDA	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 21 / 25

materials; preventing the radioactive release and damage to the public due to the criminal action of the intruder; cooperating with the relevant department to minimize the loss caused by the relevant incident.

#### 5.6.4 Contact with Local Relevant Departments

When developing emergency handling schemes, sufficient consultation shall be carried out with the local public security department, local firefighting department and environment protection department to specify the responsibilities of each department. The scheme shall be filed with the local public security department.

#### 5.6.5 Emergency Drill

The drill based on the emergency handling scheme shall be carried out annually. The drill shall focus on defence, evacuation, rescue and the coordination of the actions of various departments. Drill record and post-drill evaluation and summary shall be made.

### 27.5 Methodology for the Identification of Vital Areas

The methodology adopted in the identification of vital areas on a nuclear power plant is a critical component in determining the level of protection the nuclear security system needs to consider; the protection objectives include two parts:

- a) Nuclear materials stored in nuclear power plants and radioactive storage facilities, including the storage of new nuclear fuel components and spent fuel components,
- b) Critical equipment that may lead to radioactive release after the destruction of the core.

Nuclear materials and radioactive storage facilities on nuclear power plants need to be properly classified according to their material characteristics. The material properties mainly include elements, isotopes, quantities and levels of radiation. The specific principle of quantitative division should be based on regulatory requirements and determine the level of protection required for different nuclear materials according to the required quantitative division principle.

For critical equipment that can lead to radioactive release of the core after being damaged, it is necessary to assess the damage to these objects under various conditions, including internal and external events, and to analyse the importance of the corresponding system or equipment to the core melt or radioactive release in order to confirm the protected level of the system or device.

According to the results of Probabilistic Safety Assessment (PSA) analysis of nuclear power plants, the key systems and equipment affecting the core melting and radioactive release of nuclear power plants can be identified. This part of the system and equipment can be divided into two categories according to their function:

- a) System and equipment that will cause the nuclear power plant's originating incident after being damaged,

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 22 / 25

- b) System and equipment that will not cause the nuclear power plant's originating incident after being damaged but affect the ability to mitigate the incident.

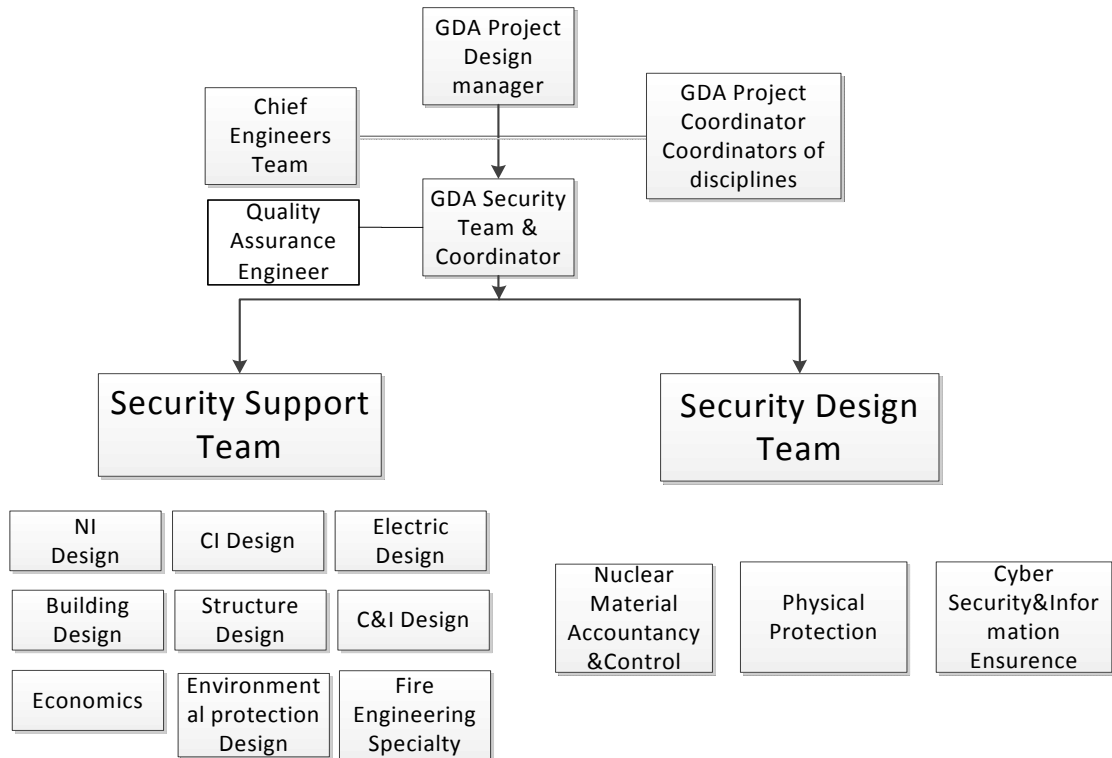
For the above-mentioned equipment, it is necessary to determine the level of protection required by PSA analysis for the contribution of the originating event to the Core Damage Frequency (CDF) or the Mass Release Frequency (MRF) of the radiation to identify the vital area.

For the above-mentioned class B equipment, the ability to mitigate the accident is judged by the PSA analysis, and the degree of protection required by the loss of the system or equipment resulting in the increased risk of core damage or radioactive release is determined to identify the vital area.

According to the results of HRP1000 preliminary PSA, several pieces of key equipment and the related systems that need to be protected in nuclear power plants can be listed. These pieces of important equipment are located in the nuclear island fuel plant, electrical plant, reactor plant, core auxiliary plant, the island connected to the plant and Safety Plant Water Pump Room, the protection and control Centre as the core part of the physical protective system, with the Nuclear Island a key zone and BPW Pump station key areas at the same time as key areas for, Reference [11].

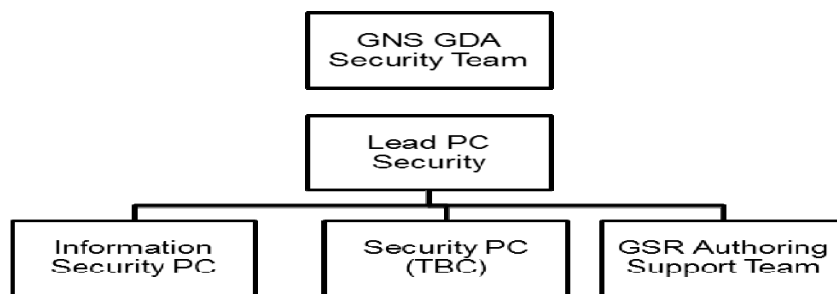
## **27.6 CGN Security Design & Technical Team**

HPR1000 GDA Project Physical Protection Specialist Group is from the Design Institute of CGNPC. The team's capability and competency covers the areas of , construction, nuclear island layout, conventional layout, structure, hydraulic technology, hydraulic structure, primary electrical system, secondary electrical system, high pressure, technical and economic, environmental protection, fire, HVAC, communications and so on.



F-27.6-1 the Physical Protection Team Structure within CNPDC

The current GNS GDA GSR team structure is as below. The team is UK based and links into the CGN team through the respective areas through both the direct counterpart as well as through the Lead PC to the GDA Security Team & Coordinator.



F-27.6-2 the Current GNS GDA GSR Team Structure

## 27.7 Conclusion

Chapter 27 provides visibility of the process and content of the NNSA assessment for HPR1000 in China and a simple summary of the ONR's regulatory requirements for nuclear security. There are also a number of security considerations that have been made during Step 1 as highlighted below:

- Access and security of offices which GNS activities will be based on what has been included in the specification for premises. The premises with security and access

<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 24 / 25

will be restricted to personnel working within the organization with appropriate arrangements for visitors.

- GNS staff will go through appropriate security vetting as standard in line with measures taken by other nuclear new build businesses.
- Information generated by GNS will carry an appropriate security marking to guide the process applied for access, handling, storage and disposal.
- Systems and facilities (electronic and physical) will be available to support the management of information from GNS generated during GDA and for media from the parent organizations.

A separate submission covering the GSR will be developed during the course of the GDA (during Steps 1 and 2) and this will cover all the detailed requirements for a security assessment of the UK HPR1000. The NSSP is a licensing requirement and is not part of the GDA GSR delivery requirement. IT and cyber security will be considered as a cross cutting issue linked to the development of I&C systems. The end product, the approved GSR, is the baseline document for the licensee's NSSP.

## **27.8 References**

- [1] ONR, A guide to nuclear regulation in the UK, October 2013.
- [2] ONR, Guidance on the Purpose, Scope and Quality of a NSSP, CNS-TAST-GD-001 Revision 0, January 2013.
- [3] China, Physical Protection for Nuclear Facilities, Nuclear Safety Guide HAD501/02.
- [4] IAEA, IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Revision 5.
- [5] NRC, CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS, RG 1.152, Revision 3, July 2011.
- [6] SC, Safety regulations for the protection of People's Republic of China computer information system, February 1994.
- [7] NDRC, Regulation of protection for power plant monitoring system of safety protection system, September 2014.
- [8] ONR, Nuclear Industries Security Regulations, September 2003.
- [9] ONR, Guidance On The Assessment Of A Duty Holder's Security Performance, CNS-TAST-GD-015 Revision 0, August 2014.
- [10] ONR, Security Assessment Principles for the Civil Nuclear Industry, 2017 Edition, Version 0.



<b>UK HPR1000 GDA</b>	Preliminary Safety Report Chapter 27 Security	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 25 / 25

[11] IAEA, IAEA Nuclear Security Series No. 16, Identification of Vital Areas at Nuclear Facilities.