

Revision	Approved by	Number of Pages
000		48
Approval Date		
 <b>General Nuclear System Ltd.</b>		
<b>UK HPR1000 GDA Project</b>		
Document Reference:	HPR/GDA/PCSR/0004	
<b>Title:</b>  <p style="text-align: center;"><b>Pre-Construction Safety Report</b></p> <p style="text-align: center;"><b>Chapter 4</b></p> <p style="text-align: center;"><b>General Safety and Design Principles</b></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 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>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 1 / 45

## TABLE OF CONTENTS

<b>4.1 List of Abbreviations and Acronyms .....</b>	<b>3</b>
<b>4.2 Introduction .....</b>	<b>4</b>
4.2.1 Chapter Route Map .....	4
4.2.2 Chapter Structure .....	7
4.2.3 Interfaces with Other Chapters .....	8
<b>4.3 Applicable Codes and Standards .....</b>	<b>10</b>
4.3.1 Codes and Standards Applied in HPR1000 (FCG3) .....	10
4.3.2 Codes and Standards Applied in UK HPR1000 .....	11
<b>4.4 General Safety and Design Principles .....</b>	<b>12</b>
4.4.1 Nuclear Safety Objective .....	12
4.4.1.1 Fundamental Safety Objective .....	12
4.4.1.2 As Low as Reasonably Practicable .....	12
4.4.1.3 Radiation Safety Requirement .....	12
4.4.2 The Concept of Defence in Depth .....	15
4.4.3 Safety Analysis .....	17
4.4.3.1 The Scope of Analysis .....	17
4.4.3.2 Deterministic Safety Analysis .....	17
4.4.3.3 Probabilistic Safety Assessment .....	21
4.4.4 Identification of Safety Functions .....	22
4.4.4.1 Fundamental Safety Functions and Decomposition of Safety Functions ..	22
4.4.4.2 Application of Safety Functions to Safety Measures .....	23
4.4.5 Categorisation of Safety Functions and Classification of Structures, Systems and Components .....	24
4.4.5.1 Categorisation of Safety Functions .....	25
4.4.5.2 Classification of Systems, Structures, and Components .....	29

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 2 / 45

4.4.5.3 Design Requirements.....	31
4.4.6 Engineering Substantiation .....	34
4.4.6.1 Design for Reliability .....	35
4.4.6.2 Design to Ensure Functionality .....	39
4.4.7 Codes and Standards .....	43
<b>4.5 Concluding Remarks .....</b>	<b>44</b>
<b>4.6 References .....</b>	<b>44</b>

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 3 / 45

## 4.1 List of Abbreviations and Acronyms

ALARP	As Low As Reasonably Practicable
AOO	Anticipated Operational Occurrence
BSL	Basic Safety Level
BSO	Basic Safety Objective
DBC	Design Basis Condition
DEC	Design Extension Condition
DEC-A	Design Extension Condition A
DEC-B	Design Extension Condition B
DiD	Defence in Depth
DSA	Deterministic Safety Analysis
EMIT	Examination, Maintenance, Inspection and Testing
EUR	European Utility Requirement
GDA	Generic Design Assessment
HAD	Chinese Nuclear Safety Guide
HAF	Chinese Nuclear Safety Regulation
HBSC	Human-Based Safety Claim
HPR1000 (FCG3)	Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
LOOP	Loss of Offsite Power
MSQA	Management of Safety and Quality Assurance
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (US)
ONR	Office for Nuclear Regulation (UK)
OPEX	Operating Experience

UK HPR1000 GDA	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 4 / 45

PCSR	Pre-Construction Safety Report
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
RG	Regulatory Guide (US)
RGP	Relevant Good Practice
SFC	Single Failure Criterion
SFP	Spent Fuel Pool
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide (UK)
UK HPR1000	UK version of the Hua-long Pressurised Reactor
URD	Utility Requirements Document (US)
WENRA	Western European Nuclear Regulators Association

## 4.2 Introduction

The main objective of this chapter is to present General Safety and Design Principles used in the design and assessment of UK version of the Hua-long Pressurised Reactor (UK HPR1000). These principles are developed based on internationally recommended good practice with consideration of UK context, more details are presented in *General Safety Requirements* in Reference [1].

### 4.2.1 Chapter Route Map

The *Fundamental Objective* of UK HPR1000 is that: *The Generic UK HPR1000 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.*

To underpin this objective, five high level claims (Level 1 claims) and a number of Level 2 claims are developed and presented in Chapter 1. This chapter supports the *Claim 2.3* derived from Level 1 *Claim 2*.

*Claim 2: The UK HPR1000 design will be developed in an evolutionary manner, using robust design process, building on relevant good international practice, to achieve a strong safety and environmental performance.*

*Claim 2.3: Suitable General Safety and Design Principles are in place to ensure the design meets the nuclear safety objective.*

To support *Claim 2.3*, this chapter develops a number of relevant arguments and

UK HPR1000 GDA	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 5 / 45

evidence:

a) **Argument 1:** *The Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) is designed based on Chinese nuclear regulatory requirements and international good practice. UK HPR1000 General Safety and Design Principles are developed from HPR1000 (FCG3) principles with the consideration of UK context.*

1) **Evidence 1:** The principles used in the design and assessment of HPR1000 (FCG3) have been demonstrated to comply with Chinese nuclear regulatory requirements. The HPR1000 (FCG3) principles are also developed based on International Atomic Energy Agency (IAEA) safety standards. In the development of HPR1000 (FCG3), the conceptual design has passed IAEA Generic Reactor Safety Review. Furthermore, other internationally recommended good practice are also considered, such as Western European Nuclear Regulators Association (WENRA) safety reports, Regulatory Guide (RG) from Nuclear Regulatory Commission (NRC), European Utility Requirement (EUR) and Utility Requirements Document (URD).

2) **Evidence 2:** The UK HPR1000 General Safety and Design Principles are developed based on the HPR1000 (FCG3) principles, reflecting the UK context and regulatory expectations, such as *Health and Safety at Work etc. Act 1974*, Reference [2], *Safety Assessment Principles for Nuclear Facilities*, Reference [3], and a series of Technical Assessment Guides (TAGs).

Moreover, Relevant Good Practice (RGP), Operating Experience (OPEX) and experience from other Generic Design Assessment (GDA) projects are also considered.

b) **Argument 2:** *Adequate and suitable General Safety and Design Principles are developed with a logical process to be applied to the design to achieve the nuclear safety objective.*

**Evidence:** *The principles are formulated based on a logical process as follows:*

- Nuclear Safety Objective is set in the design of UK HPR1000.

Nuclear safety objective is based on the fundamental safety objective presented in IAEA safety standards and the expectation of UK regulators. In order to meet the nuclear safety objective, radiation safety requirements are formulated based on the numerical targets provided in *Safety Assessment Principles for Nuclear Facilities*, Reference [3], and it is required to reduce risk to a level that is As Low As Reasonably Practicable (ALARP). The content is presented in Sub-chapter 4.4.1.

- Defence in Depth (DiD) is implemented primarily through the

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 6 / 45

combination of a number of consecutive and independent levels of protection to protect the workers and the public.

International consensus is that the appropriate strategy of preventing accidents and mitigating the consequences of accidents for achieving the nuclear safety objective is the application of the concept of DiD. In accordance with Reference [4], DiD is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects would be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier can still be available. The content is presented in Sub-chapter 4.4.2.

- Safety Analysis is carried out in UK HPR1000 to support a demonstration that the level of nuclear safety risk meets the nuclear safety objective.

Comprehensive safety analysis to assess the integrity and adequacy of levels of DiD, using a range of complimentary techniques appropriate to the level(s) in question, is the recognised good practice in demonstrating nuclear safety in design. The safety analysis is used to derive specific requirements on the safety measures. The content is presented in Sub-chapter 4.4.3.

- The safety functions are identified for ensuring a structured and comprehensive implementation of safety requirements in design.

The methodology to identify the safety functions and the safety measures (engineering and administrative) which deliver the functions is recognised good practice for ensuring a structured and comprehensive implementation of safety requirements in design. The content is presented in Sub-chapter 4.4.4.

- Safety classification of Structures, Systems and Components (SSC) is provided to establish a link between the importance of a safety function and the level of reliability and quality of SSCs that perform the safety functions.

The classification of SSCs related to safety functions is based on their role in achieving the function. The content is presented in Sub-chapter 4.4.5.

- Engineering substantiation of the safety measures is applied to ensure that the safety measures satisfy the requirements identified by safety analysis.

Engineering substantiation is applied to ensure that the safety measures

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 7 / 45

deliver the requirements (including support to the safety functions), in the conditions identified by the safety analysis, with an appropriate level of reliability according to the classification of the SSCs. The content is presented in Sub-chapter 4.4.6.

- The selection of applicable codes and standards is carried out to ensure that the reliability of SSCs is commensurate with classification of SSCs.

The selection principles and the selection process of codes and standards ensure that SSCs are designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained based on applicable codes and standards to make the reliability of SSCs commensurate with the importance of the safety function delivered by SSCs. The content is presented in Sub-chapter 4.4.7.

#### **4.2.2 Chapter Structure**

This chapter presents the General Safety and Design Principles to apply to the design and assessment of UK HPR1000. The structure of Chapter 4 is as follows:

- a) Sub-chapter 4.1 List of Abbreviations and Acronyms.

This sub-chapter lists the abbreviations and acronyms used in the chapter.

- b) Sub-chapter 4.2 Introduction.

This sub-chapter presents the purpose and scope of Chapter 4:

- 1) Sub-chapter 4.2.1 presents the claim, arguments and evidences for Chapter 4;
- 2) Sub-chapter 4.2.2 presents the structure of Chapter 4;
- 3) Sub-chapter 4.2.3 presents interfaces between Chapter 4 and other chapters.

- c) Sub-chapter 4.3 Applicable Codes and Standards.

This sub-chapter presents the applicable codes and standards for this chapter.

- d) Sub-chapter 4.4 General Safety and Design Principles.

This sub-chapter presents the General Safety and Design Principles:

- 1) Sub-chapter 4.4.1 presents the nuclear safety objective, the requirement that risk is reduced to be ALARP and radiation safety requirement in terms of radiation protection targets;
- 2) Sub-chapter 4.4.2 presents the concept of DiD reflected through all safety related activities for UK HPR1000;
- 3) Sub-chapter 4.4.3 presents the principles for safety analysis of UK HPR1000 which supports the demonstration that the level of nuclear safety risk meets

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 8 / 45

the nuclear safety objective;

- 4) Sub-chapter 4.4.4 presents the principles for identification, decomposition and application of the safety functions;
  - 5) Sub-chapter 4.4.5 presents the principles of safety classification for SSCs and relevant safety requirements;
  - 6) Sub-chapter 4.4.6 presents the engineering substantiation principles to meet the safety requirements, including Single Failure Criterion (SFC), diversity, independence, etc.;
  - 7) Sub-chapter 4.4.7 presents the selection principles of applicable codes and standards for engineering substantiation of SSCs for their reliability.
- e) Sub-chapter 4.5 Concluding Remarks.  
This sub-chapter presents the concluding remarks for this chapter.
- f) Sub-chapter 4.6 Forward Action Plan.  
This sub-chapter presents all the forward actions.
- g) Sub-chapter 4.7 References.  
This sub-chapter lists all the references cited in this chapter.

### 4.2.3 Interfaces with Other Chapters

The interfaces between this chapter and other chapters in Pre-Construction Safety Report (PCSR) are presented in T-4.2.3-1.

T-4.2.3-1 Interfaces between Chapter 4 and Other Chapters in PCSR

PCSR Chapter	Interfaces
Chapter 1 Introduction	Chapter 4 provides arguments and evidences to support the Level 2 Claim 2.3 presented in Chapter 1.
Chapter 5 Reactor Core	Chapters 5 to 11 present the design of systems and components which is based on the relevant safety and design principles provided in Chapter 4.
Chapter 6 Reactor Coolant System	
Chapter 7 Safety Systems	
Chapter 8 Instrumentation and Control	
Chapter 9 Electric Power	
Chapter 10 Auxiliary Systems	

<b>UK HPR1000 GDA</b>	<b>Pre-Construction Safety Report Chapter 4 General Safety and Design Principles</b>	<b>UK Protective Marking: Not Protectively Marked</b>	
		Rev: 000	Page: 9 / 45

<b>PCSR Chapter</b>	<b>Interfaces</b>
Chapter 11 Steam and Power Conversion System	
Chapter 12 Design Basis Condition Analysis	Chapter 12 presents the analysis of Design Basis Condition (DBC) which is based on the safety analysis principles set in Chapter 4.
Chapter 13 Design Extension Conditions and Severe Accident Analysis	Chapter 13 presents the Design Extension Condition (DEC) analysis which is based on the safety analysis principles set in Chapter 4.
Chapter 14 Probabilistic Safety Assessment	Chapter 14 presents Probabilistic Safety Assessment (PSA) which is based on the safety analysis requirements set in Chapter 4.
Chapter 15 Human Factors	Chapter 15 presents the substantiation of human factors principles which are presented in Chapter 4.
Chapter 16 Civil Works & Structures	Chapter 16 presents the design of civil works and structures which is based on the relevant principles in Chapter 4.
Chapter 17 Structural Integrity	Chapter 17 demonstrates the structural integrity by developing the design requirements that are based on the relevant principles presented in Chapter 4.
Chapter 18 External Hazards	Chapter 18 provides the methodology for protection of external hazards with the consideration of relevant principles presented in Chapter 4.
Chapter 19 Internal Hazards	Chapter 19 provides the methodology for protection of internal hazards with the consideration of relevant principles presented in Chapter 4
Chapter 20 MSQA and Safety Case Management	Chapter 20 presents codes and standards applied in Management of Safety and Quality Assurance (MSQA) which is based on the selection principles of codes and standards in Chapter 4. The organisational arrangements and quality assurance arrangements set out in Chapter 20 are implemented in the design process and production of Chapter 4.
Chapter 21 Reactor Chemistry	Chapter 21 presents codes and guidelines applied in chemistry based on the selection principles of codes and standards provided in Chapter 4.
Chapter 22 Radiological Protection	Chapter 22 presents the design of radiological protection based on the radiation safety requirements set in Chapter 4.
Chapter 23 Radioactive Waste Management	Chapters 23, 28 present the design of systems and components containing radioactive materials which is based on the safety and design principles provided in Chapter 4.
Chapter 28 Fuel Route and Storage	

PCSR Chapter	Interfaces
Chapter 24 Decommissioning	Chapter 24 presents codes and guidelines applied in decommissioning based on the selection principles of codes and standards provided in Chapter 4.
Chapter 25 Conventional Safety and Fire Safety	Chapter 25 presents applicable codes and standards in conventional safety and fire safety which are compliant with the selection principles of codes and standards provided in Chapter 4.
Chapter 29 Interim Storage of Spent Fuel	Chapter 29 presents applicable codes and standards in interim storage of spent fuel which are based on the selection principles of codes and standards provided in Chapter 4.
Chapter 30 Commissioning	Chapter 30 provides the commissioning programme for different systems and components, which considers the relevant principles presented in Chapter 4.
Chapter 31 Operational Management	Chapter 31 uses the relevant engineering substantiation principles presented in Chapter 4 to develop the operational management for UK HPR1000.
Chapter 32 Emergency preparedness	Chapter 32 presents the emergency preparedness required by principles in Chapter 4.
Chapter 33 ALARP Evaluation	Chapter 33 presents the ALARP evaluation to support and assess the achievement of the nuclear safety objective provided in Chapter 4

### 4.3 Applicable Codes and Standards

The applicable codes and standards of the principles presented in Chapter 4 are selected and determined based on the *General Principles for Application of Laws, Regulations, Codes and Standards*, Reference [5]. The principles applied in UK HPR1000 are developed from HPR1000 (FCG3) with the consideration of UK context. The analysis of applicability of the codes and standards of UK HPR1000 are presented in Sub-chapter 4.3.1 and 4.3.2.

#### 4.3.1 Codes and Standards Applied in HPR1000 (FCG3)

The principles in the design of HPR1000 (FCG3) are mainly developed from Chinese codes and standards and IAEA safety standards.

The Chinese codes and standards followed by HPR1000 (FCG3) are mainly Chinese Nuclear Safety Regulation (HAF) series such as HAF 101 (Safety Regulation on Site Evaluation for Nuclear Power Plants), HAF 102 (Safety Regulation on Design of Nuclear Power Plants) and their supporting guides the Chinese Nuclear Safety Guide (HAD) series. The HAF and HAD series are mainly based on related IAEA safety standards with consideration of Chinese regulatory requirements.

The IAEA safety standards are considered during the HPR1000 (FCG3) design process. In the development of HPR1000 (FCG3), the conceptual design has passed

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 11 / 45

IAEA Generic Reactor Safety Review. The IAEA safety standards are internationally recognised and designed to ensure a high level of safety in the use of nuclear materials and radiation sources around the world. Many member states of IAEA have decided to adopt the IAEA safety standards for use in their national regulations. The standards are also applied by designers around the world to improve the nuclear and radiation safety level in nuclear power plant.

WENRA is an internationally recognised association of the heads of Nuclear Regulatory Authorities of the European Union countries with Nuclear Power Plants (NPPs) and Switzerland which commits to a continuous improvement of nuclear safety. To develop a harmonised approach to nuclear safety and radiation protection and their regulation, WENRA produces safety reports. These reports contribute to improvement of national nuclear safety requirements. The related reports are also considered in the process of the principles formulation, such as *Safety of New NPP Designs, Safety Reference Levels for Existing Reactors*.

Furthermore, EUR and URD are also referred in the design. Though they are not codes and standards, the requirements set in them represent the expectation of utilities and are worth considering.

#### **4.3.2 Codes and Standards Applied in UK HPR1000**

The principles in UK HPR1000 are developed from HPR1000 (FCG3) and also reflect UK context.

The IAEA safety standards and WENRA safety reports that are applied to the design of HPR1000 (FCG3) are RGPs that are recognised by Office for Nuclear Regulation (ONR).

To suit UK context, *Health and Safety at Work etc. Act 1974*, Reference [2], *Tolerability of Risk from Nuclear Power Stations*, Reference [6], *Reducing Risks, Protecting People*, Reference [7], *Safety Assessment Principles for Nuclear Facilities*, Reference [3], TAGs and RGPs, such as IEC 61226, Reference [8], RCC-E, Reference [9] are considered in the development of the principles of UK HPR1000.

The main codes and standards applied in the chapter are listed in T-4.3.2-1.

T-4.3.2-1 Main Codes and Standards Applied in Chapter 4

<b>No.</b>	<b>Codes and Standards</b>
1	IAEA, Fundamental Safety Principles, No.SF-1, November 2006.
2	IAEA, Safety of Nuclear Power Plants: Design, No.SSR-2/1, Revision 1, February 2016.
3	IAEA, Deterministic Safety Analysis for Nuclear Power Plants, No.SSG-2, 2009.
4	IAEA, Safety Classification of Structures, Systems and Components in Nuclear

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 12 / 45

No.	Codes and Standards
	Power Plants, No.SSG-30, May 2014.
5	IAEA, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, May 2016.
6	IAEA, Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-TECDOC-1787, April 2016.
7	WENRA, Safety of New NPP Designs, March 2013.
8	WENRA, Safety Reference Levels for Existing Reactors, September 2014.

## 4.4 General Safety and Design Principles

### 4.4.1 Nuclear Safety Objective

The nuclear safety objective in UK HPR1000 is as follows, which is also defined as Claim 3 in PCSR Chapter 1:

*The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defence to fulfil the fundamental safety functions, reducing the nuclear safety risks to a level that is as low as reasonably practicable.*

#### 4.4.1.1 Fundamental Safety Objective

In accordance with the *Fundamental Safety Principles* of IAEA, Reference [10], the fundamental safety objective of UK HPR1000 is to protect people and the environment from harmful effects of ionising radiation. The nuclear safety objective is consistent with the fundamental safety objective of UK HPR1000 and based on the requirements of the *Health and Safety at Work etc. Act 1974*, Reference [2].

#### 4.4.1.2 As Low as Reasonably Practicable

Based upon the requirements of the *Health and Safety at Work etc. Act 1974*, Reference [2], as expressed in *Reducing Risks, Protecting People*, Reference [7] and the nuclear industry specific application in *Tolerability of Risk from Nuclear Power Stations*, Reference [6], it is necessary to show that the nuclear safety risks to the workers and the public are ALARP. This requires that all reasonable measures are taken in the design, construction and operation of the plant to minimise the radiation dose received by workers and public, unless such measures involve disproportionate sacrifice.

The ALARP methodology and evaluation are provided in Chapter 33.

#### 4.4.1.3 Radiation Safety Requirement

In order to judge the adequacy of radiological hazards control and the ALARP

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 13 / 45

assessment of risks as presented in the nuclear safety objective, radiation safety requirement is proposed. A number of dose and frequency targets for normal operation, fault and accident condition, including legal limits, are provided in *Safety Assessment Principles for Nuclear Facilities*, Reference [3]. Radiation protection targets in UK HPR1000 are set according to Reference [3].

Each target is set in terms of a Basic Safety Level (BSL) and a Basic Safety Objective (BSO). The BSLs will be met in the first place, especially the mandatory legal limits. The region under BSO represents the broadly acceptable region. The ALARP assessment will be performed to determine whether there exist reasonably practicable measures to further reduce the risk.

#### 4.4.1.3.1 Radiation Protection Targets for Normal Operation

##### a) On-site Radiation Protection Targets for Normal Operation

The UK HPR1000 targets for on-site radiation protection for normal operation are consistent with Numerical Target 1 and Target 2 set in Reference [3].

The targets and a legal limit for effective dose in a calendar year for any person on the site from sources of ionising radiation are:

##### 1) Employees working with ionising radiation:

BSL: 20 mSv (Legal Limit);

BSO: 1 mSv.

##### 2) Other employees on the site:

BSL: 2 mSv;

BSO: 0.1 mSv.

The targets for average effective dose in a calendar year to defined groups of employees working with ionising radiation are:

BSL: 10 mSv;

BSO: 0.5 mSv.

##### b) Off-site Radiation Protection Target for Normal Operation

The UK HPR1000 targets for off-site radiation protection for normal operation are consistent with Numerical Target 3 set in Reference [3].

The target and a legal limit for effective dose in a calendar year for any person off the site from sources of ionising radiation originating on the site are:

BSL: 1 mSv (Legal Limit);

BSO: 0.02 mSv.

#### 4.4.1.3.2 Radiation Protection Targets for Fault and Accident Condition

##### a) On-site Radiation Protection for Fault and Accident Condition

The UK HPR1000 targets for on-site radiation protection for fault and accident condition are consistent with on-site target in Numerical Target 4, Target 5 and Target 6 set in Reference [3].

The targets for the effective dose received by any person on the site arising from a design basis fault sequence are:

BSL:

20 mSv for initiating fault frequencies exceeding  $1 \times 10^{-3}$  pa;

200 mSv for initiating fault frequencies between  $1 \times 10^{-3}$  pa and  $1 \times 10^{-4}$  pa;

500 mSv for initiating fault frequencies between  $1 \times 10^{-4}$  pa and  $1 \times 10^{-5}$  pa.

BSO: 0.1 mSv.

The targets for the individual risk of death to a person on the site, from accidents at the site resulting in exposure to ionising radiation, are:

BSL:  $1 \times 10^{-4}$  pa;

BSO:  $1 \times 10^{-6}$  pa.

The targets for the predicted frequency of any single accident in the facility, which could give doses to a person on the site, are as presented in T-4.4.1-1.

T-4.4.1-1 Frequency Dose Targets for Any Single Accident - Any Person on the Site

Effective Dose(mSv)	Predicted Frequency Per Annum	
	BSL	BSO
2~20	$1 \times 10^{-1}$	$1 \times 10^{-3}$
20~200	$1 \times 10^{-2}$	$1 \times 10^{-4}$
200~2000	$1 \times 10^{-3}$	$1 \times 10^{-5}$
> 2000	$1 \times 10^{-4}$	$1 \times 10^{-6}$

##### b) Off-site Radiation Protection Targets for Fault and Accident Condition

The UK HPR1000 targets for off-site radiation protection for fault and accident condition are consistent with off-site target in Numerical Target 4, Target 7 and Target 8 set in Reference [3].

The targets for the effective dose received by any person off the site arising from a design basis fault sequence are:

BSL:

1 mSv for initiating fault frequencies exceeding  $1 \times 10^{-3}$  pa;

10 mSv for initiating fault frequencies between  $1 \times 10^{-3}$  pa and  $1 \times 10^{-4}$  pa;

100 mSv for initiating fault frequencies between  $1 \times 10^{-4}$  pa and  $1 \times 10^{-5}$  pa.

BSO: 0.01 mSv.

The targets for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation, are:

BSL:  $1 \times 10^{-4}$  pa;

BSO:  $1 \times 10^{-6}$  pa.

The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site, are as presented in T-4.4.1-2.

T-4.4.1-2 Frequency Dose Targets for Accidents on an Individual Facility - Any Person off the Site

Effective Dose(mSv)	Total Predicted Frequency Per Annum	
	BSL	BSO
0.1~1	1	$1 \times 10^{-2}$
1~10	$1 \times 10^{-1}$	$1 \times 10^{-3}$
10~100	$1 \times 10^{-2}$	$1 \times 10^{-4}$
100~1000	$1 \times 10^{-3}$	$1 \times 10^{-5}$
>1000	$1 \times 10^{-4}$	$1 \times 10^{-6}$

c) Overall Radiation Protection Target for Fault and Accident Condition

The target of UK HPR1000 for overall radiation protection for fault and accident condition is consistent with Numerical Target 9 set in Reference [3].

The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation, are:

BSL:  $1 \times 10^{-5}$  pa;

BSO:  $1 \times 10^{-7}$  pa.

**4.4.2 The Concept of Defence in Depth**

The concept of DiD applied in the design of UK HPR1000 is described as five levels based on the Reference [3] with consideration of UK context:

- a) The purpose of the first level is to prevent abnormal operation and failures by design. The barrier for the purpose is conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels;
- b) The purpose of the second level is to prevent and control abnormal operation and

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 16 / 45

detection of failures. This second level of defence necessitates control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures;

- c) The purpose of the third level is to control faults within the design basis to protect against escalation to an accident. This level requires engineered safety features, multiple barriers and accident or fault control procedures;
- d) The purpose of the fourth level is to control severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents. This is achieved by additional measures and procedures to protect against or mitigate fault progression and for accident management;
- e) The purpose of the fifth level is to mitigate radiological consequences of significant releases of radioactive material. This requires the provision of emergency control and on-site and off-site emergency response.

To implement the concept of DiD, successive physical barriers are in place to confine radioactive material at specified locations. Three barriers are as follows:

- a) Barrier 1: Fuel cladding;
- b) Barrier 2: Reactor coolant pressure boundary;
- c) Barrier 3: Containment building.

According to Reference [11], the concept of DiD for UK HPR1000 is considered not only as the requirement to achieve a number of consecutive barriers and levels of protection, but also as general principle for the formulation of safety requirements, including requirements of the achievement of quality and reliability for barriers and systems to ensure their capability.

As far as reasonably practicable, independence between different levels of DiD are considered, which means that if one level were to fail, the fault sequence can be terminated by a subsequent level. The following presents the independence between levels to be provided in the UK HPR1000 design:

- a) To the extent practicable, SSCs used in Level 1 and Level 2 of DiD are independent from SSCs designed for the protection in Level 3;
- b) To the extent practicable, SSCs designed for Level 3 are independent from SSCs for Level 4;
- c) To the extent practicable, SSCs specifically designed to mitigate consequences of severe accidents in Level 4 of DiD are independent from other levels of DiD.

The means to achieve the independence between SSCs are described in Sub-chapter 4.4.6.

### 4.4.3 Safety Analysis

To provide assurance that DiD has been appropriately implemented in the design of the plant, safety analysis is carried out using a number of complementary techniques to support a demonstration that the level of nuclear safety risk meets the nuclear safety objective.

The safety analysis for UK HPR1000 is based on the IAEA approach in Reference [4], using the Deterministic Safety Analysis (DSA) methodology combined with PSA.

#### 4.4.3.1 The Scope of Analysis

In the design of the plant, it is recognised that challenges to all levels of DiD may occur and design measures need to be provided to ensure that the necessary safety functions are accomplished and the safety objectives can be met. These challenges stem from the Postulated Initiating Events (PIEs).

The PIEs considered include all foreseeable failures of SSCs of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states, in the reactor, the spent fuel pool or other systems containing radioactive or fissile material.

Besides the occurrence of PIE, there may be consequential effects caused by the PIE which are considered as a part of the original PIE. The combinations of randomly occurring individual events are evaluated using appropriate screening criteria to ensure that credible coincident events are considered in the design.

Where PIEs are excluded from the deterministic analysis, and in some cases from the probabilistic analysis (being beyond design basis or not credible), a comprehensive technically supported justification shall be provided.

The identified PIEs are common inputs for both DSA and PSA. More details about methodology of PIE identification are provided in Reference [12].

#### 4.4.3.2 Deterministic Safety Analysis

In the design of UK HPR1000, the plant states are considered in DSA. Plant states which are shown in T-4.4.3-1 are identified and grouped into a limited number of categories primarily on the basis of their frequency of occurrence and consequence.

T-4.4.3-1 Plant States

Operational States		Accident Conditions		
Normal operation	Anticipated Operational Occurrences (AOOs)	Design basis accidents	Design Extension Conditions	
			Without significant fuel degradation	With core melting (severe accidents)

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 18 / 45

The plant states can be subdivided into 4 categories of DBC and 2 categories of DEC. The DSA is carried out with the analysis of DBC and DEC.

a) Design Basis Condition

The DBC is classified into 4 categories according to its frequency and good practice from other projects or standards: DBC-1, DBC-2, DBC-3, and DBC-4.

Based on the UK context, they can also be classified into frequent faults and infrequent faults.

b) Design Extension Condition

The DEC is classified into 2 categories:

- 1) Design Extension Condition A (DEC-A): DEC events without significant fuel degradation;
- 2) Design Extension Condition B (DEC-B): DEC events with core melting.

Details about the plant state list for UK HPR1000 are provided in Reference [13].

The plant states including DBCs and DECs are considered within the concept of DiD. T-4.4.3-2 provides a comparison between the IAEA, UK HPR1000 and UK context terminologies to better understand the relationship between the plant states of UK HPR1000 and the level of DiD.

T-4.4.3-2 Overview of UK Context, UK HPR1000 and IAEA Terminology

IAEA terminology		Plant State	UK HPR1000 Plant State	Frequency (pa) <sup>1</sup>	UK Context Terminology (based on Reference [3])		
DiD Level	Description				Plant State	DiD Level (used in UK HPR1000)	Description
1	Prevention of abnormal operation and failures	Normal Operation	DBC-1	$IFF \geq 1$	Normal operation	Prevention of abnormal operation and failures by design	1
2	Control of abnormal operation and detection of failures	Anticipated Operational Occurrences	DBC-2 <sup>2</sup>	$1 > IFF > 10^{-2}$		Prevention and control of abnormal operation and detection of failures	2
3a	Control of design basis accidents	Design Basis Accidents	DBC-3 <sup>3</sup>	$10^{-2} > IFF > 10^{-3}$	Frequent faults	Control of faults within the design basis to protect against escalation to an accident	3
			---	$10^{-3} > IFF > 10^{-4}$			
			DBC-4	$10^{-4} > IFF > 10^{-5}$			
3b	Control of design extension conditions to prevent core melt	Design Extension Conditions	DEC-A <sup>4</sup>	$IFF > 10^{-3}$ and $FSF > 10^{-7}$	Frequent fault + failure of 1 <sup>st</sup> line of protection	Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents	4
4	Control of design extension conditions to mitigate the consequences of severe accidents		DEC-B	---	Beyond design basis conditions (including severe accident)		
5	Mitigation of radiological consequences of significant releases of radioactive materials	Accident with releases requiring implementation of emergency countermeasures	N/A	---	Off-site emergency	Mitigation of radiological consequences of significant releases of radioactive material	5

Notes:

1. IFF: Initiating Fault Frequency, FSF: Fault Sequence Frequency;
2. DBC-2 corresponds to abnormal operation before a fault (UK context level 2 of DiD), and to frequent faults where there is a demand on a safety system (UK context Level 3 of DiD);
3. DBC-3 corresponds to faults at the lower end of frequent fault range, and at the higher end of infrequent fault range;
4. Although DEC-A is considered as design extension condition under IAEA terminology, for UK HPR1000 it includes the scenario of a diverse line of protection against frequent faults and is therefore within the UK context design basis when used for this purpose. DEC-A may also be used to represent conditions beyond the UK context design basis, but before DEC-B (severe accident).

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 20 / 45

Appropriate assumptions are considered in the DSA to ensure the adequacy of safety measures. Further detailed information about DSA is provided in PCSR Chapters 12 and 13:

a) The analysis of DBC-2, DBC-3, DBC-4 applies conservative methodology at an appropriate (high) confidence level. The analysis assumptions for DBC-2, DBC-3, DBC-4 based on Reference [14] are as follows:

- 1) For the purpose of conservative calculations, the initial and boundary conditions are set to values that will lead to conservative results for those safety parameters that are to be compared with the acceptance criteria;
- 2) The single failure criterion is applied when determining the availability of systems and components. A failure is assumed in the system or component that would have the largest negative effect on the calculated safety parameter;
- 3) All the common cause and consequential failures associated with the PIE are also included in the analysis, in addition to the single failure;
- 4) Equipment that is not qualified for specific accident conditions is assumed to fail unless its continued operation results in more unfavourable conditions;
- 5) The time interval between detection of the abnormal event or accident and the required action is sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) are specified to ensure the performance of such actions;
- 6) Loss of Offsite Power (LOOP) due to turbine trip shall be considered for DBC-2, DBC-3 and DBC-4 accidents at power if it is conservative;
- 7) Preventive maintenance for safety systems is not considered.

Further explanation of items 1 to 6 is presented in PCSR Chapter 12. Further explanation of maintenance states and maintenance philosophy versus operating mode is presented in PCSR Chapter 31.

b) The analysis of DEC-A applies best estimate methodology. The analysis assumptions for DEC-A are as follows:

- 1) Key initial parameters, main system parameters and time delay are considered with conservative assumptions;
- 2) Single failure and consequential LOOP are not considered;
- 3) Equipment that is not qualified for specific accident conditions is assumed to fail unless its continued operation results in more unfavourable conditions;
- 4) The time interval between detection of the abnormal event or accident and the required action is sufficiently long and adequate procedures (such as

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 21 / 45

administrative, operational and emergency procedures) are specified to ensure the performance of such actions;

- 5) Preventive maintenance for safety systems is not considered.

Further explanation of items 1 to 4 is presented in PCSR Chapter 13. Further explanation of maintenance states and maintenance philosophy versus operating mode is presented in PCSR Chapter 31.

c) Safety Criteria

The safety criteria are defined to ensure that the safety objective is met. The safety criteria are addressed in Sub-chapter 4.4.1.2, and the decoupling criteria are presented in Chapter 12 and 13.

4.4.3.3 Probabilistic Safety Assessment

In the frame of the UK HPR1000 design process, PSA studies are to demonstrate that a balanced design of UK HPR1000 has been achieved such that no particular feature or PIE makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of DiD are independent. It provides assurance that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff edge effects) will be prevented, and compares the results of the analysis with the acceptance criteria for risk where these have been specified, Reference [4].

The UK HPR1000 PSA covers:

- a) All sources of radioactivity present at the facility, including the reactor core, spent fuel, radioactive wastes and new fuel. The PSA for the reactor core is presented in Sub-chapter 14.4, 14.5 and 14.8. The PSA for the Spent Fuel Pool (SFP) is presented in Sub-chapter 14.6 and 14.8. The PSA for radioactive wastes is presented in Sub-chapter 14.7. The analysis for new fuel is included in SFP PSA (which is presented in Sub-chapter 14.6 and 14.8.);
- b) All types of initiating events (consideration of internal events, internal hazards and external hazards). The initiating events for internal events Level 1 PSA are presented in Sub-chapter 14.4.1. Internal hazards and external hazards Level 1 PSA are presented in Sub-chapter 14.4.2;
- c) All plant operational states for reactor core and SFP. The operational states for reactor core are presented in Sub-chapter 14.4.1, the operational states for SFP are presented in Sub-chapter 14.6.5;
- d) Identification of the sequence of events that can lead to core damage and estimation of the core damage (Level 1 PSA), identification of ways in which radioactive releases from the plant can occur and estimation of their magnitude and frequency (Level 2 PSA), estimation of public health and other societal risks

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 22 / 45

(Level 3 PSA), more details are presented in Sub-chapter 14.4, 14.5 and 14.8.

PSA is applied to demonstrate that the safety objective can be met and to justify the design of the nuclear power plant is balanced. The PSA provides an important insight into the UK HPR1000 design and supports decision-making during the design of UK HPR1000. During the GDA process, the development of the PSA enables the identification of the potential design vulnerabilities that contribute most significantly to the risk. PSA is also used to analyse the risk impact associated with potential design improvements, and to understand the important contributors. The detailed PSA approach is provided in PCSR Chapter 14.

#### **4.4.4 Identification of Safety Functions**

The three fundamental safety functions which are defined in IAEA No. SSR-2/1 (Rev.1) *Safety of Nuclear Power Plants: Design*, Reference [4], are fulfilled for all plant states in UK HPR1000, and they are top-level safety functions for UK HPR1000.

To facilitate the development of the technical design, the three fundamental safety functions are developed into several levels of functions defined in more detail which are specific to the design and the assessment of the plant. The decomposition of safety functions follows a systematic and comprehensive methodology and process which are implied to ensure the sufficiency and completion of safety functions.

##### **4.4.4.1 Fundamental Safety Functions and Decomposition of Safety Functions**

The fundamental safety functions for the NPP are described as following based on good practice in Reference [4]:

- a) R: Control of reactivity;
- b) H: Removal of heat from the reactor and from the fuel store;
- c) C: Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

In UK HPR1000 design, there is an additional type of function named “Extra Safety Functions”, which consists of supporting functions and hazard prevention, protection and mitigation functions.

These fundamental safety functions have been further developed into high level safety functions based on Reference [15], [16], [17] and taking into account the UK HPR1000 design features. The high level safety functions are:

- a) Control of reactivity
  - 1) R1: Maintain core reactivity control;

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 23 / 45

- 2) R2: Shutdown and maintain core sub-criticality;
  - 3) R3: Prevention of uncontrolled positive reactivity insertion into the core;
  - 4) R4: Maintain sufficient sub-criticality of fissile material stored outside the reactor coolant system but within the site.
- b) Removal of heat
- 1) H1: Maintain sufficient Reactor Coolant System water inventory for core cooling;
  - 2) H2: Remove heat from the core to the reactor coolant;
  - 3) H3: Transfer heat from the reactor coolant to the ultimate heat sink;
  - 4) H4: Maintain heat removal from fuel stored outside the RCS but within the site.
- c) Confinement
- 1) C1: Maintain integrity of the fuel cladding to ensure confinement of radioactive material;
  - 2) C2: Maintain integrity of the Reactor Coolant Pressure Boundary to ensure confinement of radioactive material;
  - 3) C3: Maintain integrity of reactor containment to ensure confinement of radioactive material;
  - 4) C4: Maintain integrity of the fuel stored outside of reactor containment;
  - 5) C5: Store the radioactive material;
  - 6) C6: Shield against radiation, control planned radioactive releases, and limit accidental radioactive releases.
- d) Extra safety functions
- 1) E1: Support Type R, H or C safety function;
  - 2) E2: Prevent, protect and mitigate hazards impact.

The High Level Safety Functions are developed more specifically into low level safety functions, and then applied in safety system design.

Further information about the safety functions are presented in *Decomposition of Safety Functions*, Reference [18].

#### 4.4.4.2 Application of Safety Functions to Safety Measures

Where the high level safety functions are decomposed to low level safety functions, taking account of the plant design and operating modes, the low level safety functions

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 24 / 45

identified are allocated to the technical means or measures for the purpose of achieving the functional requirements.

Each high level function (R, H, C or E) is decomposed into low level safety functions or a set of functions, all of which are required for the high level function to be achieved in that particular circumstance. The SSCs providing a low level safety function are then identified. It is important to note that:

- a) A single system (means) may support more than one low level function, for different faults;
- b) A single low level function may be supported by multiple systems (means);
- c) Supporting systems (essential services such as component cooling, power supply, air supply, etc.) are identified that are necessary for the delivery of a function by the claimed means;
- d) Supporting indications are identified that are necessary or complementary for the delivery of a function by the claimed means, depending whether the systems are manually or automatically initiated. Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

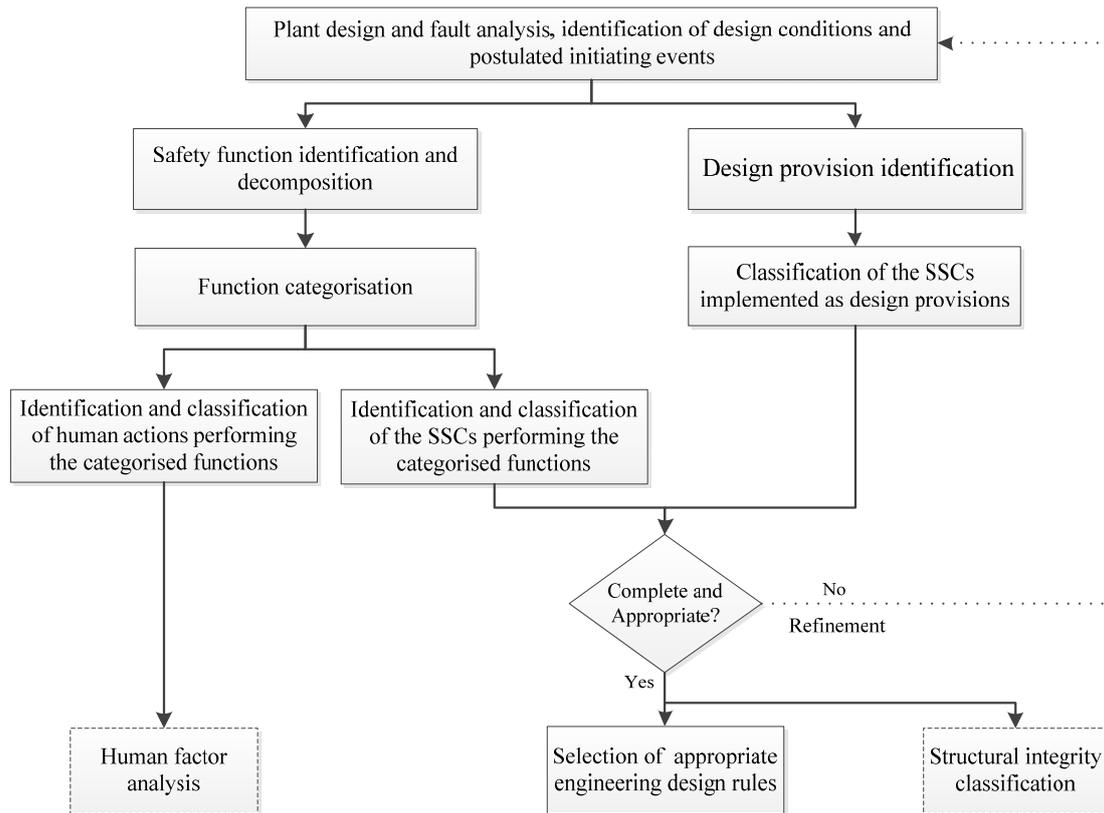
The safety requirements on a system to be substantiated (see Sub-chapter 4.4.5) are derived based on the low level safety function(s) to be provided in order to remain within the appropriate DiD levels (normal operating or design basis limit), and on the conditions under which the functions are to be provided, at the appropriate reliability.

#### **4.4.5 Categorisation of Safety Functions and Classification of Structures, Systems and Components**

Safety classification of SSCs provides a link between the significance of a safety function and the level of reliability and quality of the SSCs that are needed to perform the safety function to protect people and the environment from harmful effects of ionising radiation.

The UK HPR1000 safety categorisation and classification approach is based on IAEA Safety Standard No.SSG-30, Reference [19], and relevant technical documents IAEA-TECDOC-1787, Reference [17], NS-TAST-GD-094, Reference [20], and IEC 61226, Reference [8], are also taken into account.

Classification is a top-down process that is based on an adequate understanding of the plant design, fault analysis and how to achieve the fundamental safety functions. This process is illustrated in F-4.4.5-1.



#### F-4.4.5-1 Safety Categorisation and Classification Process Overview

##### 4.4.5.1 Categorisation of Safety Functions

The classification of SSCs related to safety functions is based on their role in achieving the function. The categorisation of safety functions are based on the considerations as follows:

- a) The consequences of failure to perform the safety function;
- b) The frequency of the occurrence of the PIEs for which the function will be called upon;
- c) The plant states that the function contributes to reaching after an initiating event.

The potential radiological consequences of failure are graded as High, Medium or Low as an input to categorisation and classification. The rating of High, Medium or Low is directly related to safety category. For UK HPR1000, the High, Medium and Low are defined as follows:

- a) For off-site releases:
  - 1) High consequences are defined as a release of radioactive material that exceeds the BSL of off-site radiation protection targets for fault and accident condition (correspond to Numerical Target 4 in Reference [3]) presented in Sub-chapter 4.4.1.3.2;

- 2) Medium consequences are defined as a release of radioactive material that exceeds the limits of normal operation for faults with initiating fault frequency greater than  $10^{-4}$  pa, or exceeding 1mSv for faults with initiating fault frequency less than  $10^{-4}$  pa;
  - 3) Low consequences are below the limits of normal operation. For the UK context, this is interpreted as a release greater than the BSO of off-site radiation protection targets for fault and accident condition (correspond to Numerical Target 4 in Reference [3]) presented in Sub-chapter 4.4.1.3.2.
- b) For on-site releases:
- 1) High consequences are defined as a dose to an individual on site exceeding 200mSv for faults with initiating fault frequency  $\geq 10^{-3}$  pa (frequent faults), or exceeding 500 mSv for faults  $< 10^{-3}$  pa (infrequent faults);
  - 2) Medium consequences are defined as a dose to an individual on site exceeding 2 mSv for faults with initiating fault frequency greater than  $10^{-4}$  pa, or exceeding 20 mSv for faults with initiating fault frequency less than  $10^{-4}$  pa;
  - 3) Low consequences are defined as a dose to an individual on site exceeding the BSO but below 2 mSv for faults with initiating fault frequency greater than  $10^{-4}$  pa, or below 20 mSv for faults with initiating fault frequency less than  $10^{-4}$  pa.

The contribution that the functions make in reaching the plant states after an initiating event is considered for the categorisation of safety functions. For DBCs, the plant states include controlled state and safe state. For DECAs, there is no distinction made between the controlled and safe state, hence the designation of final state is used.

The definition of controlled state and safe state is described in T-4.4.5-1.

#### T-4.4.5-1 Characteristics of Controlled State and Safe State

	<b>For Reactor Core</b>	<b>For Spent Fuel</b>
<b>Controlled State</b>	<ul style="list-style-type: none"> <li>• the core is subcritical</li> <li>• heat removal is assured for a time sufficient to implement provisions to reach a safe state, e.g. via steam generators</li> <li>• coolant inventory is stable</li> <li>• radioactive release meets regulatory limits</li> </ul>	<ul style="list-style-type: none"> <li>• fuel storage is subcritical</li> <li>• water level is stabilised and the water inventory is adequate for spent fuel cooling and shielding</li> <li>• radioactive release meets regulatory limits</li> </ul>
<b>Safe State</b>	<ul style="list-style-type: none"> <li>• the core is subcritical</li> <li>• residual heat removal is assured on a long term basis, e.g. via</li> </ul>	<ul style="list-style-type: none"> <li>• fuel storage is subcritical</li> <li>• water level is stabilised and the water inventory is</li> </ul>

	<b>For Reactor Core</b>	<b>For Spent Fuel</b>
	residual heat removal heat exchanger <ul style="list-style-type: none"> <li>reactor coolant inventory is recovered</li> <li>radioactive releases are controlled and acceptable</li> </ul>	adequate for spent fuel cooling and shielding <ul style="list-style-type: none"> <li>spent fuel pool cooling is established on a long term basis</li> <li>radioactive releases are controlled and acceptable</li> </ul>

A controlled state is therefore considered to be a stable and safe state in the analysis of the reactor as the key safety significant parameters identified above will be shown to be stable. A safe state is considered to be maintaining a stable, safe state. The controlled state and safe state of DBC is also applied to the analysis of diverse line. For DEC's the final state is considered to be maintaining a stable and safe state.

The initial categorisation of functions under different plant states in the UK HPR1000 nuclear power plant is shown in T-4.4.5-2 for Level 1 DiD, T-4.4.5-3 for Level 2 DiD, and T-4.4.5-4 for Level 3, 4 and 5 DiD. Note that UK HPR1000 uses the terminology FC1, 2, 3 and NC to indicate Cat1, 2, 3 and Non-Categorised.

T-4.4.5-2 Function Categorisation for Level 1 of DiD

<b>DiD Level</b>	<b>Context of Function</b>	<b>Severity of the Consequences if the Function is not Performed</b>		
		<b>High</b>	<b>Medium</b>	<b>Low</b>
Consequences are assessed on the basis that Level 3 of DiD function is performed, i.e. mitigated, protected consequences		<b>DBC-1 Function Category</b>		
Level 1	Function required during DBC-1 to control a duty system, with potential to cause a fault if it fails	1 <sup>1</sup>	2	3

Notes:

- High mitigated, protected consequences implies the associated Level 3 of DiD function is ineffective, absent or bypassed by the fault, all of which are undesirable (e.g. some fuel handling faults). In such a case, it should be shown that functions provided in Levels 1 and 2 of DiD can deliver an equivalent level of safety.

T-4.4.5-3 Function Categorisation for Level 2 of DiD

DiD Level	Context of Function		Function Category
Level 2 <sup>1</sup>	Independent function which acts to prevent a fault. Provided to complement the DBC-1 function and allow its Category to be reduced by one level (Category 2 to Category 3 or Category 3 to NC)		3
	Independent function which acts to prevent a fault. Claimed to reduce fault frequency from frequent to infrequent region	Category 2 DBC-1 function or initiating event frequency (assuming failure of Level 1 DiD function) less than $10^{-2}$ pa	3
		Category 3 DBC-1 function or initiating event frequency (assuming failure of Level 1 DiD function) less than $10^{-1}$ pa	2

Notes:

- Level 2 DiD functions can either be used to complement Level 1 DiD, allowing balance in design between the integrity level of duty and preventative functions (row 1 in the Table above), or to reduce the demand on Level 3 of DiD, and hence balance the design between prevention and protection (rows 2 and 3 in the Table above). In some circumstances there may be no claimed Level 2 function.

T-4.4.5-4 Function Categorisation for Faults

DiD Level	Functions Credited in the Safety Assessment	Severity of the Consequences if the Function is not Performed		
		High	Medium	Low
Consequences are assessed on the basis that safety functions in later plant states are not performed, and that functions failed earlier in the fault sequence are not available i.e. unmitigated, unprotected consequences		<b>DBC / DEC Function Category</b>		
Level 3	Functions to reach a controlled state under DBC-2, 3 and 4 conditions	1	2	3
	Functions to reach and maintain a safe state under DBC-2, 3 and 4 conditions	2	3	3
	Functions providing a diverse backup to a Category 1 function in a frequent fault	2 <sup>1</sup>	---	---

<b>DiD Level</b>	<b>Functions Credited in the Safety Assessment</b>	<b>Severity of the Consequences if the Function is not Performed</b>		
		<b>High</b>	<b>Medium</b>	<b>Low</b>
	Functions providing a diverse backup to a Category 2 function in a frequent fault	3	---	---
Level 4	DEC-A functions with initiating fault frequency $< 10^{-5}$ pa	3	---	---
	Functions for the mitigation of severe accidents	3	---	---
Level 5	Any function relating to the monitoring needed to provide off-site emergency services, including monitoring and communication means as part of the emergency response plan	3	---	---

Notes:

1. Functions that are used in multiple failure conditions but that are not required in the short term after the onset of the accident may be assigned to Category 3 function.

#### 4.4.5.2 Classification of Systems, Structures, and Components

This sub-chapter defines the classification of SSCs providing functions, and also SSCs that are treated as a design provision.

##### 4.4.5.2.1 Classification of SSCs Providing a Categorised Function

Once the safety categorisation of the functions is completed, the SSCs performing these functions are assigned to a safety class. Through identification of system-related input data, the related SSCs which perform the categorised functions are to be identified.

All SSCs that fulfil Category 1, 2 and 3 functions must be subject to SSCs classification. The assignment of the SSCs classification is shown in T-4.4.5-5.

##### T-4.4.5-5 Safety Classification of SSCs according to Safety Function Category

<b>Function Category</b>	<b>SSC Class</b>
Category 1	Class 1
Category 2	Class 2
Category 3	Class 3

Note that UK HPR1000 uses the terminology F-SC1, 2, 3 and NC to indicate Functional Class 1, 2, 3 and Non-Classified.

If an SSC fulfils multiple functions, its classification depends on a function with the highest function categorisation.

Human actions that are required to perform or to support a safety function are classified based on the significance of the safety function similar to SSCs.

#### 4.4.5.2.2 Classification of Design Provisions

Categorisation of the functions provided by design provisions is not necessary because the safety significance of the SSC can be directly derived from the consequences of its failure. The consequences of failure are graded as High, Medium or Low which are defined in Sub-chapter 4.4.5.1. The SSCs implemented as design provisions can therefore be directly assigned to a safety class without the need for a further analysis of safety function categories.

Design provisions are classified directly based on their consequences of failure according to T-4.4.5-6 below.

#### T-4.4.5-6 Classification of Design Provisions

<b>Context of Function</b>	<b>Severity of the Consequences if the Design Provision Fails</b>		
	<b>High</b>	<b>Medium</b>	<b>Low</b>
Consequences of failure of design provisions during normal operation are assessed on the basis that safety functions in Level 3 of DiD are performed, i.e. mitigated, protected consequences			
Design provision whose failure could lead directly to radiological release during normal operation (DPH, DPM, DPL correspond to High, Medium and Low consequences)	Class 1	Class 2	Class 3
Consequences of failure of design provisions during faults are assessed without benefit from later levels of DiD. If the failure of the SSC also affects an active function then the function category are also considered.			
Design provision whose failure could lead to radiological release during a fault (DPA) due to loss of containment of radioactive material.	Class 1	Class 2	Class 3

Note that UK HPR1000 uses the terminology B-SC1, 2, 3 and NC to indicate Design Provisions Class 1, 2, 3 and Non-Classified.

#### 4.4.5.2.3 Classification of Structural Integrity

On the basis of safety classification, the structural integrity classification is also taken

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 31 / 45

into account to be consistent with UK context expectation. The structural integrity classification for UK HPR1000 is presented in PCSR Chapter 17.

#### 4.4.5.3 Design Requirements

Engineering design rules are the relevant national or international codes, standards and proven engineering practices that are applied, as appropriate, to the design of SSCs to meet the applicable design requirements.

A complete set of engineering design rules are specified to ensure that the SSCs could be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained to appropriate quality standards. To achieve this, the design rules identify appropriate levels of capability, reliability (dependability) and robustness. The design rules also take due account of regulatory requirements relevant to safety classified SSCs.

##### 4.4.5.3.1 General Design Requirements

Practically, capability and reliability of systems performing a categorised function are achieved by meeting design requirements relevant for the safety class of the system. The contents of the requirements include:

- a) Single failure criterion;
- b) Physical and electrical separation;
- c) Emergency power supply;
- d) Periodic test;
- e) Environmental qualification;
- f) Protection against internal and external hazards (including earthquakes).

The general design requirements for systems are shown in T-4.4.5-7.

T-4.4.5-7 System Design Requirements

<b>System Classification</b>	<b>Single Failure Criterion <sup>1</sup></b>	<b>Physical and Electrical Separation</b>	<b>Emergency Power Supply</b>	<b>Periodic Test <sup>5</sup></b>	<b>Environmental Qualification <sup>7</sup></b>	<b>Protection Against Internal and External Hazards (Including Earthquakes)</b>
F-SC1	Yes <sup>1</sup> System level	Yes	Yes	Yes	Yes	Yes
F-SC2	Yes <sup>2</sup> Function level	Yes <sup>3</sup>	Yes	Yes	Yes	Yes
F-SC3	No	Special requirements <sup>4</sup>	Case by case	Yes <sup>6</sup>	Case by case	Case by case

Notes:

1. Consideration of single failure criterion at the “system level” of F-SC1 systems indicates that these systems must be redundant;
2. Consideration of single failure criterion at the “function level” for F-SC2 systems indicates that these systems may not need redundancy. When a system is subject to non-redundant design, another system must fulfil the same function (functional diversity) and single failure evaluation on it must be performed. In this case, physical isolation requirements should be applied on multiple pipelines of different systems fulfilling the same function. A F-SC2 system is not required to meet single failure criterion if it performs a function that provide a backup to a Category 1 function and that is required to control DEC-A conditions;
3. For redundant system or function diversity series;
4. F-SC3 systems require to be separated from F-SC1 and F-SC2 systems, especially from functions and systems at different DiD level, according to analysis results of internal and external hazards;
5. Active safety systems must be designed so that periodic testing can be performed;
6. Except for the case where continuous operation is required;
7. Qualification requirements are determined according to the specific equipment operational environment. In particular, equipment performs Category 3 functions that copes with DECAs should meet requirements for environmental radioactivity, pressure, temperature, etc. in the corresponding DECAs.

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 33 / 45

#### 4.4.5.3.2 Relationship between Classes and Design Codes and Standards

The high level principle for system design requirements is that Class 1 and Class 2 systems are designed in accordance with nuclear specific codes and standards, where those are available. Class 3 systems may be designed in accordance with nuclear specific or industrial codes and standards.

Selection of specific codes and standards is carried out in accordance with relevant good practice for the particular engineering topic area. The selection principle of applicable codes and standards is presented in Sub-chapter 4.4.7 and detailed application of codes and standards are presented in relevant chapters.

#### 4.4.5.3.3 Seismic Requirements

Two seismic categories are defined: seismic category 1 (SSE1) and seismic category 2 (SSE2). Non-seismic is designated as NO.

Generally, seismic requirements are divided into four categories as follows:

- a) Operability (O): Ability of an active component (including all the necessary auxiliary systems, supporting systems and energy supply systems) to fulfil its safety functions and thus meet the safety objective;
- b) Functional capacity (F): Ability of all parts of components (active and passive) to withstand the specified loadings such deformations occurring in these components are limited so that their safety function is not impaired;
- c) Integrity (I): Ability of active and passive components to withstand the specified loadings at the given frequency of occurrence throughout the service life of the component;
- d) Stability (S): Ability of an active or passive component to withstand loads that tends to change its orientation or position (for instance, causing it to sway, fall or slide unacceptably, or causing parts to shear). Component stability includes, among other things, the necessary resistance and stability of its supports.

#### 4.4.5.3.3.1 Seismic Category 1 (SSE1)

The seismic category of Class 1 and Class 2 items is SSE1. SSCs that are determined as Class 3 are not usually categorised as SSE1, unless specifically required by the safety analysis of the seismic event. Important examples of SSE1 from Class 3 include:

- a) Class 3 systems required to allow the reactor or spent fuel to reach a safe state under DEC-A conditions;
- b) Class 3 systems claimed for severe accident management (DEC-B);
- c) Isolation, detection and fire-fighting systems in the buildings containing

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 34 / 45

mechanical, electrical or Instrumentation and Control (I&C) equipment that fulfil FC1 and FC2 functions;

- d) Some systems with additional functions (FC3) that are essential to maintain a safe state but which may be required in the period between 24 and 72 hours;
- e) Parts of the process information and control system.

Generally speaking, for SSE1 electrical and I&C components, “operability” during and after an earthquake is required; for SSE1 mechanical components, “functional capacity” or “operability” after an earthquake is required.

Any equipment actuated (such as certain valves, reactor automatic trip and shutdown) or in operation (such as F-SC1 system pumps) during an earthquake, “operability” during the earthquake is required.

#### 4.4.5.3.3.2 Seismic category 2 (SSE2)

The seismic category of non-SSE1 SSCs are SSE2 if any internal hazards caused by failure of the SSCs in a seismic event resulting from an earthquake could cause an unacceptable effect on SSE1 SSCs. This could include the following consequential hazards.

- a) Toppling or falling on to SSE1 equipment;
- b) Generation of missiles;
- c) Effects resulting from failure of high-energy equipment;
- d) Flooding resulting from failure of fluid systems;
- e) Explosion;
- f) Fire.

If SSCs are claimed to limit the effect of a hazard caused by a seismic event, they must also be suitably categorised as SSE2 at least. Consideration is given to the possibility of multiple failures resulting from the effect of an earthquake in the analysis of earthquake induced accident consequences. Secondary failure resulting from failure of electrical and I&C equipment must be prevented by electrically isolating protected and unprotected systems.

More detailed information of safety categorisation and classification is presented in Reference [21].

#### **4.4.6 Engineering Substantiation**

The nuclear safety principles in Sub-chapter 4.4.1 to Sub-chapter 4.4.5 ensure that the fault analysis could identify safety measures and corresponding safety requirements suitable to meet the overall nuclear safety objective.

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 35 / 45

The safety requirements on SSCs are substantiated to satisfy the appropriate reliability in accordance with their classification requirements. The envelope defined by the aggregate safety requirements on a system represents the system design basis, aligned with the definition in Reference [11].

This sub-chapter provides the generic principles to be applied in substantiating that safety measures are able to meet the safety requirements placed on them (fulfilling the design basis), and to identify any operational and maintenance activities that will be required to underpin the engineering substantiation.

#### 4.4.6.1 Design for Reliability

##### 4.4.6.1.1 Application of the Hierarchy of Risk Reduction to the Design

The design of the plant and of individual safety measure reflects the preferences identified in the hierarchy of risk reduction, as far as reasonably practicable:

- a) Inherent safety: The design avoids radiological hazards rather than controlling them. The potential for harm is eliminated by design;
- b) Fault tolerance: A PIE produces no safety significant effects or produces only a change towards safe plant conditions by means of inherent characteristics of the plant;
- c) Passive safety: Following a PIE, the plant should be rendered safe by means of passive safety features or by the action of systems that are operating continuously in a state necessary to control the PIE;
- d) Engineered safety systems: Following a PIE the plant should be rendered safe by the actuation of safety systems that need to be brought into operation in response to the PIE. In general, automatically acting systems are preferred to those that require manual initiation;
- e) Administrative procedures: Following a PIE, the plant should be rendered safe by specified procedures.
- f) Mitigation safety measures: Filtration, scrubbing, etc.

##### 4.4.6.1.2 Single Failure Criterion and Redundancy

The reliability of items important to safety is commensurate with their safety significance. According to Reference [4], the single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

The single failure includes active and passive failures:

- a) An active single failure is defined as a failure which is sufficient to invalidate the relevant safety function of a component, including the malfunction of a

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 36 / 45

mechanical or electrical component which relies on mechanical movement to complete its intended function upon demand, and the malfunction of an I&C component;

- b) A passive single failure is defined as a failure which could occur in a component that does not change its state while realising its function.

The single failure criterion is applied to each safety group considered in fault analysis. A single failure of active component within systems that deliver FC1 or FC2 safety functions is required to be tolerated at or after the PIE, when their action is demanded. A single failure of passive components within systems that deliver FC1 or FC2 safety functions need to be assessed at the start of a transient in an appropriate means.

The considerations about the single failure criterion are as follows:

- a) FC1 function, F-SC1 system: provide redundancy within the system to ensure tolerance to a single failure;
- b) FC2 function, F-SC2 system: provide redundancy within the system, or provide at function level by multiple systems capable of providing the same function, to ensure tolerance to single failure;
- c) FC3 function, F-SC3 system: may not provide redundancy, although may be necessary to achieve the reliability under the fault sequence in question.

It should be noted that a F-SC2 system that belongs to a diverse protection line is not required to consider the single failure criterion in the system design.

In some cases, if one train of a safety system fails due to an initiating fault and the second train fails taking single failure criterion into account, then the third redundancy train is needed to ensure that the required safety function is reliably performed.

The design of UK HPR1000 will ensure reliability during maintenance by redundancy design and management procedures. For preventive maintenance, the activities can be managed through adequate planning and compensatory measures in maintenance procedures. These activities are not arranged in the condition when the function is needed in DBC fault sequences analyses. For corrective maintenance, it is managed by compensatory measures and recovery time and plant fall-back modes according to operating limits and conditions. If the duration is inadequate to recover the function, it is performed when the plant is under a condition where the function is not required.

#### 4.4.6.1.3 Independence

In addition to the high level principle of independence between levels of DiD, the following principles for independence are applied in the design to achieve system reliability and to have tolerance to faults:

- a) Independence between trains of redundant system components is maintained as

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 37 / 45

far as reasonably practicable (avoidance of common cause failure);

- b) Independence between components of different safety classes is maintained as far as reasonably practicable (avoidance of impact on the component of higher safety class from an item of lower safety class);
- c) Independence between components designed to mitigate a potential initiating event and the effects of this potential initiating event is maintained as far as reasonably practicable;
- d) Independence between SSCs important to safety and those not important to safety is maintained as far as reasonably practicable.

Independence is accomplished in the design of systems by using functional isolation and/ or physical separation. Functional isolation is used to reduce adverse effects between elements of connected systems or systems redundantly designed. These adverse effects may be caused by the normal operation, abnormal operation or failure of any part of these systems.

Interference between protection systems and control systems are prevented by avoiding interconnection or by appropriate isolation measures. If signals are shared by a protection system or any control system, isolation measures will be ensured and it will be demonstrated that the design still meet all the safety requirements of protection systems.

Physical separation are applied in the layout of systems as far as reasonably practicable, to reduce the potential of common cause failure due to a localised initiating event. The choice of isolation measures (compartmentalisation, distance, orientation etc.) takes into account the nature of the initiating events.

#### 4.4.6.1.4 Diversity

The design of equipment takes due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

Diversity is realised by incorporating different attributes into redundant systems or components. Such attributes can be different operating principles, different physical variables, different operating conditions, different manufacturers, etc.

The concept of diversity is taken into consideration in the realisation of a safety function to reduce the risk in the case during the loss of the first protection line. In UK HPR1000 design, a diverse protection line is designed to protect or mitigate frequent faults.

The analysis rules applied for the diverse protection line are as follows:

- a) Key initial parameters, main system parameters and time delay are considered with conservative assumptions;
- b) Single failure and consequential LOOP are not considered;
- c) Equipment that is not qualified for specific accident conditions is assumed to fail unless its continued operation results in more unfavourable conditions;
- d) The time interval between detection of the abnormal event or accident and the required action is sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) are specified to ensure the performance of such actions;
- e) Preventive maintenance for safety systems is not considered.

The Categorisation requirements for the diverse protection line of UK HPR1000 are presented in T-4.4.6-1.

T-4.4.6-1 Categorisation of Diverse Protection Line

First Protection Line functions	Diverse Protection Line functions
FC1	FC2
FC2	FC3
FC3	---

#### 4.4.6.1.5 Fail-safe Design

The fail-safe design is considered and incorporated, as appropriate, into the design of systems and components important to safety of UK HPR1000, so that their failure or the failure of a support feature will not invalidate the performance of the intended safety function.

Spurious operation and unsafe failure modes of systems and components are considered in the design. Priority is given to predictable and revealed failure modes during equipment selection.

#### 4.4.6.1.6 Human Factors

A systematic approach needs to be applied to identify the factors that affect human performance and minimise the potential for human error throughout the entire plant lifecycle.

The design allocates functions properly, support personnel in the fulfilment of their responsibilities and in the performance of their tasks. The design also needs to

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 39 / 45

identify human actions that may affect safety and proportionately analyse all tasks important to safety and limit the likelihood of operational errors and their impact on safety.

A systematic approach to human factor integration is established and applied throughout the entire lifecycle of UK HPR1000, especially at the design stage.

Human factor integration covers the plant locations where operations and maintenance activities take place. To comply with the requirements above, the following elements are met:

- a) The design allocates functions properly to minimise the dependence on human actions;
- b) Human actions that could impact safety during normal operation, fault and accident conditions are identified systematically. These human actions important for safety are known as Human-Based Safety Claims (HBSCs);
- c) Appropriate human factor analysis, including task analysis and human reliability analysis, is performed on the HBSCs to identify potential improvements to systems, procedures or training;
- d) All HBSCs are classified either based on their risk significance or on the significance of the safety system affected;
- e) The design supports personnel in the fulfilment of their responsibilities and in the performance of tasks by providing suitable and sufficient user interfaces and workspace.

More detailed information about human factors is presented in Chapter 15.

#### 4.4.6.2 Design to Ensure Functionality

##### 4.4.6.2.1 Equipment Qualification

Equipment qualification is implemented to verify that items important to safety are capable of performing their intended functions when necessary, and in the environmental conditions (including the variations in ambient environmental conditions) that are anticipated in the design for the plant. In order to achieve this objective, the operating conditions considered for equipment qualification includes DBCs and DEC.

Equipment qualification includes:

- a) Environmental qualification: to verify the performance of the equipment in the normal and accidental environmental conditions;
- b) Seismic qualification: to verify the performance of the equipment during or after an earthquake.

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 40 / 45

Considering the results of fault analysis and the safety classifications, the specific equipment to be qualified is listed as follows:

- a) Equipment required for environmental qualification
  - 1) Mechanical equipment and electrical equipment that perform FC1 or FC2 functions;
  - 2) Mechanical equipment and electrical equipment that perform FC3 functions, which are required:
    - To maintain a safe state;
    - To protect against DEC-A and mitigate DEC-B.

Normal operational and accident conditions are considered in the equipment qualification process. Normal operational conditions consider the lifetime of the equipment and the environment of the normal condition in the plant where the equipment is placed. The variation of environmental condition arising from the accident conditions is considered in the environmental qualification.

- b) Equipment required for seismically qualification

The equipment that performs the following functions is seismically qualified: operability (O), functionality (F), integrity (I) or stability (S). The detailed explanation of which is presented in Sub-chapter 4.4.5.3.3.

The parameters which are related to the environmental conditions and their impact on equipment are presented below:

- a) Temperature

Temperature can indirectly change the performance of the equipment by gradual chemical and physical processes, which is also called thermal ageing.

- b) Pressure

Pressure and its rapid changes can affect the performance of equipment by exerting additional forces on the equipment. High increase of external or internal pressure may cause structural failure of fully sealed equipment. The rapid increase of pressure may cause structural failure of the imperfectly sealed equipment.

- c) Radiation

Radiation could induce changes in the atomic and molecular structure of matter through excitation, oxidation, crosslinking, degradation and shearing process, resulting in the change of equipment performance. Some changes improve the performance of the equipment, but most of the changes cause a decline in the performance.

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 41 / 45

Four main types of radiation ( $\alpha$ ,  $\beta$ ,  $\gamma$  and neutron) occur within a nuclear power plant. The  $\gamma$  radiation possesses a very strong capacity for penetration. The penetration capacity of  $\beta$  radiation is a lot less, and 1mm steel or 10 mm water layer can shield most of the  $\beta$  radiation. The penetration capacity of  $\alpha$  radiation is lower still. Neutron radiation is considered for equipment near the reactor pit.

d) Humidity

Humidity (high humidity) can directly lead to equipment performance degradation, and can make other environmental conditions worse. For example, moisture could lead to corrosion and current effects at the interfaces of different metals. Moisture could directly reduce the performance of organic materials, degrading their physical, mechanical and electrical performance and deforming them. Moisture on the surface can significantly reduce the insulation resistance and breakdown voltage of the insulator.

The methods of equipment qualification are presented below, which are determined according to Reference [9] and [22]:

- a) Type test under representative conditions, in accordance with an appropriate test standard;
- b) Qualification by analysis:
  - 1) Calculation (design analysis), usually structural load analysis and mechanical analysis in accordance with an appropriate design code;
  - 2) Operating experience based;
  - 3) Analogy - by comparison with similar qualified equipment.

Considering the specific characteristics of the equipment to be qualified, the methods listed above can be used individually or in combination.

#### 4.4.6.2.2 Ageing and Degradation

The design life of items important to safety is evaluated and defined. The power plant of UK HPR1000 is designed for 60 years. For the reactor vessel and all major structures, equipment which are not replaceable, such as the containment, the design lifetime is 60 years. Some devices are designed for 60 years, though they are replaceable. For SSCs which are not designed for 60 years, the replaceability of these SSCs is considered in the design.

The issues caused by obsolescence of SSCs, especially systems and components, are also considered. Appropriate margins are provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 42 / 45

Periodic measurement of material properties and parameters that could change with time is made to assess ageing mechanisms predicted at the design stage and to help to identify unanticipated behaviour of the plant or degradation that might occur in service.

Detailed information relating to the operational management of ageing and degradation is addressed in Sub-chapter 31.6 and the activities of ageing and degradation are presented in relevant system chapters.

#### 4.4.6.2.3 Examination, Maintenance, Inspection and Testing

The effective Examination, Maintenance, Inspection and Testing (EMIT) is essential for the safe operation of the plant. They ensure that the levels of reliability and availability of all SSC important to safety remain in accordance with the design over the lifetime of the plant.

The design of EMIT activities are facilitated for the purpose of maintaining the capability of SSC important to safety, so as to satisfy the reliability requirement. The SSCs are designed to ensure that they are maintainable, inspectable, and testable. The key aspects of considerations for EMIT are presented as follows:

- a) EMIT will be identified according to regulatory requirements, reliability analysis and potential degradation mechanisms etc.
- b) The frequency of EMIT activities, which are carried out at predetermined intervals, will be determined to reduce the probability of failure or the degradation of the SSC safety function.
- c) Type test will be considered as reference data to establish a baseline for EMIT;
- d) An unacceptable degradation of the validity of equipment qualification will be avoided when EMIT activities are carried out.
- e) EMIT activities shall be carried out according to the procedures for maintaining or checking the quality and restoring inherent levels of reliability. The procedures that include all of maintenance, periodic test, and inspection activities shall be established.
- f) The engineered measures will be provided to ensure the design is maintainable, inspectable, and testable. The key engineered measures are given as follows:
  - 1) The plant layout where the items important to safety are installed will have adequate space to prevent crowding and be designed for accessibility during EMIT activities. When the replacement of a component is needed, the plant layout design should consider the transportation and storage of the special tools and the new component;
  - 2) The means of failure detection and isolation of SSC will be provided to

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 43 / 45

enable to perform EMIT activities;

- 3) The radiation protection means in design features will be provided to ensure that the risk associated with EMIT has been reduced to be ALARP;
- 4) The environment conditions are very important to EMIT activities during the service life. Therefore, the means of environment conditions monitoring will be provided in the design phase.
- g) EMIT will be designed to avoid safety functions being made unavailable on the system being repaired, inspected, or tested, except when a safety function is not required in the specific condition. The potential to loss of a safety function for these activities should be analysed, and the risks should be justified.

A functional testing of SSC will be carried out under the conditions in which they will operate when performing their intended functions as far as possible.

- h) Following an event, necessary EMIT activities will be required to revalidate the safety functions and structural integrity of the SSC that may have been challenged.

The detailed information about the EMIT operational management is addressed in Sub-chapter 31.6 and the EMIT activities on each SSC important to safety are presented in relevant system chapters.

#### **4.4.7 Codes and Standards**

To reflect the functional reliability requirements, SSCs are designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained based on a complete set of applicable codes and standards. The design codes and standards are identified in accordance with safety classification of SSCs.

The principles for selection of applicable codes and standards are explored after comprehensively considering necessary factors that include the design characteristics, UK regulatory expectations, requirements of guidance documents, engineering practice etc. The main selection principles are provided as follows, and the selected codes and standards are:

- a) Commensurate with the categorisation of safety functions and classification of the SSCs (detail information is presented in 4.4.5);
- b) The relevant good practice recognised by regulator;
- c) The latest version.

The selection process applied includes collection, screening, assessment, justification and analysis. The applicability, adequacy and sufficiency of codes and standards are identified and evaluated, and relevant factors are also considered, such as scope of application, degree of familiarity, application in practical engineering and relationship

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 44 / 45

with the reference plant. The selection process will ensure applicable codes and standards are adopted, which is sufficient to support the design and justification.

Details of the selection principles and the process are presented in the *General Principles for Application of Laws, Regulations, Codes and Standards* in Reference [5]. The justification of suitability of codes and standards and the list of main codes and standards for specific areas are discussed in Sub-chapter X.3 of all chapters.

## 4.5 Concluding Remarks

General Safety and Design Principles in UK HPR1000 are developed from HPR1000 (FCG3) whilst considering UK context.

To achieve the nuclear safety objective, the principles are developed with a logical process as follows:

- a) Nuclear safety objective;
- b) The concept of DiD;
- c) Safety analysis;
- d) Categorisation of safety functions and classification of SSCs;
- e) Engineering substantiation;
- f) Codes and standards.

General Safety and Design Principles in UK HPR1000 are adequate, suitable and reflect UK context. These principles are applied in the design to support the reduction of the nuclear safety risks to be ALARP.

## 4.6 References

- [1] CGN, General Safety Requirements, GHX00100017DOZJ03GN, Revision C, August 2018.
- [2] The Stationery Office, The Health and Safety at Work etc. Act 1974, 1974.
- [3] ONR, Safety Assessment Principles for Nuclear Facilities, Revision 0, 2014.
- [4] IAEA, Safety of Nuclear Power Plants: Design, No.SSR-2/1, Revision 1, February 2016.
- [5] CGN, General Principles for Application of Laws, Regulations, Codes and Standards, GHX00100018DOZJ03GN, Revision F, August 2018.
- [6] Health and Safety Executive, The Tolerability of Risk from Nuclear Power Stations, 1992.
- [7] Health and Safety Executive, Reducing Risks, Protecting People, 2001.

<b>UK HPR1000 GDA</b>	Pre-Construction Safety Report Chapter 4 General Safety and Design Principles	UK Protective Marking: Not Protectively Marked	
		Rev: 000	Page: 45 / 45

- [8] IEC, Nuclear Power Plants - Instrumentation and Control Important to Safety –Classification of Instrumentation and Control Functions, IEC 61226, Edition 3.0, September 2009.
- [9] AFCEN, Design and Construction Rules for Electrical and I&C System and Equipment, RCC-E, December 2016.
- [10] IAEA, Fundamental Safety Principles, No.SF-1, November 2006.
- [11] IAEA, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, May 2016.
- [12] CGN, Methodology of PIE Identification, GHX00100008DOZJ03GN, Revision E, July 2018.
- [13] CGN, The Design Condition List and Acceptance Criteria, GHX00100029DOZJ04GN, Revision D, August 2018.
- [14] IAEA, Deterministic Safety Analysis for Nuclear Power Plants, No.SSG-2, 2009.
- [15] IAEA, Assessment of Defence in Depth for Nuclear Power Plants, Safety Report Series No. 46, February 2005.
- [16] IAEA, Storage of Spent Nuclear Fuel, No. SSG-15, February 2012.
- [17] IAEA, Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-TECDOC-1787, April 2016.
- [18] CGN, Decomposition of Safety Functions, GHX80001001DOZJ03GN, Revision C, September 2018.
- [19] IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, No.SSG-30, May 2014.
- [20] ONR, Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094, Revision 0, November 2015.
- [21] CGN, Methodology of Safety Categorisation and Classification, GHX00100062DOZJ03GN, Revision B, June 2018.
- [22] IEC/ IEEE, Nuclear Facilities – Electrical Equipment to Safety - Qualification, IEC/ IEEE 60780-323, 2016.