Revision	Approved by	Number of Pages
000		34
Approval Date	26/10-17	

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	**HPR/GDA/PSR/0004**

Preliminary Safety Report

Chapter 4

General Safety and Design Principles

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).

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.

DISTRIBUTION LIST

Recipients	Cross Box
GNS Executive	☐
GNS all staff	☐
GNS and BRB all staff	☒
CGN	☒
EDF	☒
Regulators	☒
Public	☐

SENSITIVE INFORMATION RECORD

Section Number	Section Title	Page	Content	Category

Table of Contents

4.1 List of Abbreviations and Acronyms

ALARP	As Low As Reasonably Practicable
CCF	Common Cause Failure
DBC(s)	Design Basis Condition(s)
DEC(s)	Design Extension Condition(s)
DEC-A	Design Extension Condition A
DEC-B	Design Extension Condition B
DiD	Defence in Depth
FPS	Fault and Protection Schedule
GB	Chinese National Standards
GDA	Generic Design Assessment
HAF	Chinese Nuclear Safety Regulations
HPR1000 (FCG3)	Hua-long Pressurized Reactor under Construction at Fangchenggang Nuclear Power Plant Unit 3
IAEA	International Atomic Energy Agency
NB	Chinese Energy Standard
NC	Non-Categorised, Non-Classified
NNSA	National Nuclear Safety Administration
NPP(s)	Nuclear Power Plant(s)
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PIE(s)	Postulated Initiating Event(s)
PSR	Preliminary Safety Report
PWR	Pressurized Water Reactor
RHR	Residual Heat Removal [RHR]
RIS	Safety Injection System [SIS]
RP	Requesting Party
SAP	Safety Assessment Principles for Nuclear Facilities

SFC	Single Failure Criterion
SG	Steam Generator
SSC(s)	Structure(s), System(s) and Component(s)
SSG	Specific Safety Guide
SSR	Specific Safety Requirements
TAG	Technical Assessment Guides
UK HPR1000	The UK version of the Hua-long Pressurized Reactor

4.2 Introduction

This chapter supports the following high level objective:

The UK version of the Hua-long Pressurized Reactor (UK HPR1000) design will be developed in an evolutionary manner, using robust design processes, building on relevant good international practice, to achieve a strong safety and environmental performance.

A robust system of codes and standards is used during the design process which supports this objective. However, the design for UK HPR1000 for the Generic Design Assessment (GDA) has not yet been declared and consequently the detailed UK HPR1000 design process has not been fully defined and the associated information about codes and standards will be available in the following design phase.

The design of UK HPR1000 will be based on the version of the Hua-long Pressurized Reactor under Construction at Fangchenggang Nuclear Power Plant Unit 3 (HPR1000 (FCG3)), whose design is driven by international good practice (e.g. international codes, standards and guidance), as discussed in Chapter 1.

At the early phase of HPR1000 development, it was decided by CGN that the general safety and design principles applied for HPR1000 would be developed in consistency with the Safety Regulations on Design of Nuclear Power Plants (HAF102-2004) which was established and approved by National Nuclear Safety Administration (NNSA) of China in April 2004. The HAF102-2004, which is basically issued in consistent with the Safety of Nuclear Power Plants: Design (IAEA safety standards No. NS-R-1, published in 2000) with some changes considering the regulatory practices of nuclear power plants (NPPs) in China, reflected the international and Chinese consensus about how to ensure safety of high level and was then considered as the best practice for new-designed NPPs in China.

After the Fukushima nuclear accident (March 2011), the General Technical Requirements for Post-Fukushima-Accident Improvement Actions of Nuclear Power Plants was established by NNSA of China in June 2012 in order to draw lessons from the Fukushima nuclear accident in Japan and further improve the safety level of nuclear power plants in China. HPR1000 was then reviewed against those requirements to confirm the relevant safety improvements required by this document had already been considered in the design of HPR1000. Thereafter similar review against Safety of Nuclear Power Plants: Design (IAEA safety standards No. SSR-2/1, Rev.0 in 2012 and Rev.1 in 2016) were conducted for ensuring the design of HPR1000 was benchmarked with international best practices.

Hereafter this chapter provides a summary of the design process followed in the development of the HPR1000 (FCG3) design that will form the basis of the processes to be followed in the development of UK HPR1000 design. This chapter will demonstrate the following:

a) The fundamental safety objective is achieved by the design of HPR1000 (FCG3);

b) The concept of defence in depth is implemented as a basic approach for ensuring safety of the plant;

c) The necessary safety functions are identified to support the performing of three fundamental safety functions of the plant;

d) The design conditions are considered in the design to establish appropriate boundary conditions that HPR1000 (FCG3) should withstand;

e) Safety functions for Structures, Systems and Components (SSCs) are identified and categorised based on their significance to safety;

f) Appropriate Codes and Standards are identified for the substantiation of the design;

g) A qualification process is implemented to ensure that SSCs perform their allocated safety function(s);

h) Design Requirements for achieving appropriate level of reliability for SSCs are defined to support the design development and substantiation.

Besides the above-mentioned objective, the following requirements will also be considered in the design for UK HPR1000. These requirements are demonstrated in several other chapters of Preliminary Safety Report (PSR).

a) The General Plant Design and Operational Envelope ensure the effects of faults and accidents are kept below specified limits as what have been demonstrated by the analyses of faults and accidents. Relevant information such as the design basis of systems and structures, and the analyses of various conditions are provided in Chapter 6~11, 16 and 12~13 respectively;

b) The design and layout facilitates access for necessary activities and minimise adverse interactions while not compromising security aspects. Relevant requirements are provided in Chapter 22 and 27;

c) The Plant Design and Operation includes provision for testing, maintaining, monitoring and inspecting SSCs to mitigate defects and the effects of ageing and degradation in order to maintain the availability and reliability. See Chapter 17 for relevant requirements and Chapter 6~11 for supportive information;

d) The plant layout (including the pipework layout) and operation limit radiation levels in areas requiring access and reduce the time personnel spend in those areas. See Chapter 22 for relevant requirements.

The purpose of this chapter is to describe the major safety and design principles which have been applied in nuclear safety related design activities associated with the development of HPR1000 (FCG3), including the principles for:

a) General safety aspects;

b) Classification for SSCs;

c) Selection of codes and standards;

d) Equipment Qualification.

This chapter discusses how the evolution of the HPR1000 (FCG3) technology supports that the HPR1000 (FCG3) design was developed using robust design processes to optimise the nuclear safety and environmental performance of the design.

This chapter also discusses how that approach will continue to be followed during the design development of UK HPR1000.

Sub-chapter 4.3 is, generally, a statement and description of the fundamental safety objective and the main nuclear safety claims of HPR1000 (FCG3). The conventional safety aspects are addressed in Chapter 25.

Sub-chapter 4.4 describes the concept of defence in depth implemented throughout the design of HPR1000 (FCG3).

Sub-chapter 4.5 describes the derivation of supporting lower level safety functions.

Sub-chapter 4.6 presents only the requirement and rationale for defining a comprehensive list of design conditions. The detail information about design conditions are presented in Chapter 12 & 13 of this PSR.

Sub-chapter 4.7 describes the Safety Classification of SSCs in HPR1000 (FCG3).

In sub-chapter 4.8, the high level codes and standards applied for HPR1000 (FCG3) are identified. There is also a commitment made concerning a theoretical benchmark for the assessment of relevant good practices for codes and standards recognised in the UK.

In sub-chapter 4.9, the principles of qualification are described, including the scope of equipment qualification and qualification methods used for HPR1000 (FCG3).

In sub-chapter 4.10, the general requirements for ensuring reliability of SSCs in HPR1000 (FCG3) are presented.

It has been recognized that there are some gaps between the design of HPR1000 (FCG3) and UK regulatory expectations, including the principles for:

a) The concept of defence in depth;

b) Design conditions;

c) Safety classification;

d) Codes and standards;

e) Design for reliability of structures, systems and components.

These gaps are described in the associated sub-chapter.

4.3 Fundamental Safety Objective

In accordance with the International Atomic Energy Agency's Fundamental Safety Principles (IAEA Safety Standards No.SF-1) in Reference [1], the fundamental safety objective of HPR1000 (FCG3) is to protect people and the environment from harmful effects of ionizing radiation. This approach will be continued for UK HPR1000 and is elucidated via the fundamental project objective that 'UK HPR1000 design will be developed in an evolutionary manner, building on relevant good international nuclear practice, using robust design processes to optimize the safety and environmental performance'.

The fundamental safety objective is achieved by the following measures which are accordance with the IAEA's Safety of Nuclear Power Plants: Design (IAEA Safety Standards No.SSR-2/1) in Reference [2]:

a) To control the radiation exposure of people and radioactive releases to the environment in operational states;

b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, spent nuclear fuel, radioactive waste or any other source of radiation at a nuclear power plant;

c) To mitigate the consequences of such events if they were to occur.

For the achievement of the fundamental safety objective above, the radiation protection design objective and the safety design objective are proposed.

4.3.1 Radiation Protection Design Objective

For the achievement of the fundamental safety objective, the radiation protection design ensures that the radiation exposure in all operational states within the plant, or due to any planned release of radioactive material from the plant, is kept below the prescribed limits and as low as reasonably achievable. Furthermore, measures have to be taken to mitigate the radiological consequences of any accidents.

4.3.2 Safety Design Objective

For the achievement of the safety design objective, the following measures could be taken which is accordance with IAEA Safety Standards No.SSR-2/1 in Reference [2]:

a) To prevent accidents with harmful consequences resulting from a loss of control over the reactor core or over other sources of radiation, and to mitigate the consequences of any accidents that do occur;

b) To ensure that for all accidents taken into account in the design of the installation, any radiological consequences would be below the relevant limits and would be kept as low as reasonably achievable;

c) To ensure that the likelihood of occurrence of an accident with serious radiological

consequences is extremely low and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable.

A comprehensive safety assessment is carried out to demonstrate that the fundamental safety objective is achieved by the design. All the possible radiation sources are identified and all potential doses that might be received by workers or public and environment are evaluated.

The radiological consequences of accidents would be reduced by taking measures to mitigate the accidents. The measures are as follows:

a) provision of safety features and safety systems;

b) establishment of accident management procedures by the operating organization;

c) establishment of off-site protective actions by the appropriate authorities.

All the event sequences leading to high radiation doses or large radioactive release would be 'practically eliminated'[1], and events of high frequency are limited so that only minor potential radiological consequences are caused by them. An essential objective for design is that no or only limited off site protection and intervention is necessary to mitigate the radiological consequences.

4.4 The Concept of Defence in Depth

For the achievement of the fundamental safety objective described above, the concept of defence in depth is implemented throughout the safety approach for HPR1000 (FCG3) which includes deterministic assessments complemented by probabilistic analyses.

The concept of defence in depth in IAEA Safety Standards No.SSR-2/1 in Reference [2] is applied for HPR1000 (FCG3) and described as five levels:

a) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety;

b) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions;

c) The third level of defence requires that inherent and/or engineered safety features, safety systems and procedures shall be capable of preventing damage to the reactor core or preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state, if an accident occurs;

d) The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth;

[1] The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.

e) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents.

The concept of defence in depth of HPR1000 (FCG3) is roughly the same with UK regulatory expectations, but there are some differences in detail. For example, a safety objective of level 4 of defence in depth in the design of HPR1000 (FCG3) is that the Design Extension Conditions (DECs) are addressed by additional safety measures rather than safety systems designed for coping with design basis accidents considered on level 3. However, there is no clear definition as 'DECs' within the concept of defence mentioned in Safety Assessment Principles for Nuclear Facilities (SAP) EKP.3.

The concept of defence in depth which will be defined for UK HPR1000 in Pre-Construction Safety Report (PCSR) will be consistent with both the recommendation of IAEA and of SAPs.

4.5 Safety Functions

Fulfilment of the following fundamental safety functions for the plant are ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Each of the fundamental safety functions consists of different high level safety functions. For instance, control of reactivity being fundamental safety function consists of maintaining core reactivity control, shutdown and maintaining core sub-criticality and so on. High level safety functions which are lower level than fundamental safety functions are different in various types of reactors.

Each of high level safety functions consists of different low level safety functions as well. For instance, maintaining core reactivity control being high level safety function consists of control of the boron concentration - slow variations, control of the reactor coolant system average temperature - power operation and so on. Low level safety functions relative to high level safety functions are different in various types of plants.

The principles above about safety functions are established mainly based on IAEA Safety Standards No.SSR-2/1 in Reference [2], with no difference between these principles and the claim of the SAP EKP.4.

4.6 Design Conditions

The design of HPR1000 (FCG3) has identified a comprehensive set of internal postulated initiating events, which consider all foreseeable events with the potential for serious consequences, all foreseeable events with a significant frequency of occurrence and operating errors. Design basis accidents grouped from postulated initiating events to establish the boundary conditions for the nuclear power plant to withstand without acceptable limits for radiation protection being exceeded.

Acceptance criteria are assigned to each category of design conditions, such that plant event sequences that could result in severe consequences are of very low probability, and plant event sequences with a significant frequency of occurrence have no, or only minor, potential radiological consequences.

A safety analysis of the design for the nuclear power plant is conducted in a way in which both deterministic analysis and probabilistic analysis are applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

In the deterministic safety analysis of HPR1000 (FCG3), two kinds of design conditions, i.e. Design Basis Conditions (DBCs) and DECs, are defined and analysed. The definition and analysis of these design conditions are discussed in Chapter 12 & 13 respectively. Generally, the analyses about DBC-2, DBC-3 and DBC-4 are related to the level 3 of defence in depth, and the analyses about Design Extension Condition A (DEC-A) which means the design extension condition without significant fuel degradation and Design Extension Condition B (DEC-B) which means the design extension condition with core melting are related to the level 4 of defence in depth.

Plant states of HPR1000 (FCG3) typically cover:

a) Normal operation;

b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;

c) Design basis accidents;

d) Design extension conditions, including accidents with core melt.

The safety analysis of HPR1000 (FCG3) includes all the following six operation modes:

a) Reactor power operation;

b) Normal shutdown/steam generator cooling;

c) Normal shutdown/RIS-RHR cooling;

d) Maintenance cold shutdown;

e) Refuelling cold shutdown;

f) Reactor completely defueled.

In accordance with Safety Assessment Principles (SAPs) established by the Office for Nuclear Regulation (ONR), the identification of safety functions for UK HPR1000 will based on a systematic analysis of normal operation to identify all Postulated Initiating Events (PIEs). Therefore a systematic process to identify the PIEs for UK HPR1000 and to develop the associated Fault and Protection Schedule (FPS) will be submitted as part of the PCSR of UK HPR1000. The FPS, once produced, will demonstrate that the engineered safety provisions provided by the SSCs designed in accordance with the

objectives identified in this chapter for UK HPR1000, to be described in the PCSR, will be sufficient to reduce the risks from UK HPR1000 to people and the environment As Low As Reasonably Practicable (ALARP).

4.7 Safety Classification

4.7.1 Overview

The safety of HPR1000 (FCG3) relies on the fulfilment of identified safety functions under all design conditions that have been defined for the plant. Therefore, the level of reliability or integrity of the SSCs which perform these safety functions should be achieved and maintained appropriately to ensure the safety of the plant.

The approach of categorisation and classification used for HPR1000 (FCG3) contributes to the objective that all SSCs are designed, manufactured, installed and operated with appropriate requirements so that their quality, reliability and integrity, being commensurate with their contribution to safety, can be achieved and maintained. Consequently, the safety of HPR1000 (FCG3) can be ensured by the functions which are performed by these SSCs.

It should be noted that the approach of categorisation and classification described in this sub-chapter, which is established mainly based on IAEA Safety Standard No.SSG-30 in Reference [3] and relevant technical documents in Reference [4] with some changes recommended by Chinese regulator or by engineering experiences of existing Chinese Nuclear Power Plants (NPPs), is only applied for HPR1000 (FCG3).

It has been noticed that an approach of categorisation and classification has been recommended by the SAP ECS.1 & ECS.2 and the classification-related Technical Assessment Guides (TAG) (NS-TAST-GD-094) in Reference [5]. Though it's announced that the approach recommended by the TAG is consistent with that of IAEA Safety Standard No.SSG-30, we have found several differences between the guidance and requirements in those two approaches (e.g. the factors considered in categorisation and classification, the criteria used in defining the category of functions, the reliability requirements or the requirements of failure frequency assigned to each SSC class etc.).

A gap analysis is being undertaken between the approach used for HPR1000 (FCG3) and those recognized as relevant good practice in UK. The approach to be applied for UK HPR1000 will be defined after the gap analysis completes and will be described in UK HPR1000 Pre-Construction Safety Report (PCSR). It will be mainly based on the approach described in this sub-chapter and the gaps will be addressed properly.

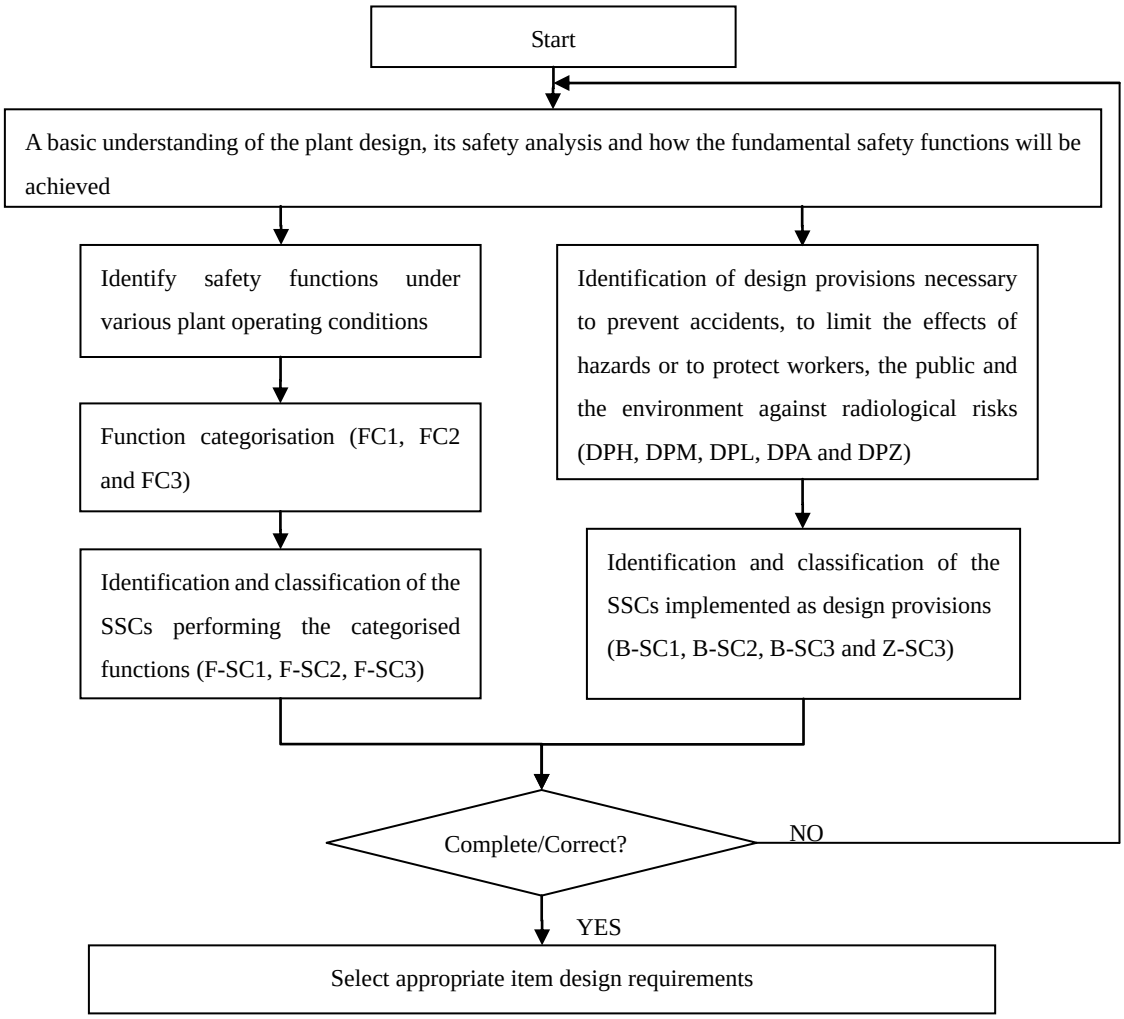
The iterative process of categorisation and classification also contributes to minimise risks ALARP.

4.7.2 Purpose and Process of Safety Classification

The safety of HPR1000 (FCG3) relies on the reliability or integrity of its SSCs. It's necessary to classify every individual SSC into a systematic hierarchy to ensure that all

SSCs are designed, manufactured, installed and operated with appropriate requirements established for HPR1000 (FCG3) so that their quality and reliability are commensurate with their safety significance and the safety of plant can be ensured by the functions which are performed by these SSCs.

In accordance with IAEA Safety Standard No.SSG-30 in Reference [3], the process for the safety classification of HPR1000 (FCG3) is shown in F-4.7-1.



F-4.7-1 Process of safety classification

The top-down process of safety classification used for HPR1000 (FCG3) consists of two parallel ways which are related to ‘Safety Functions’ and ‘Design Provisions’ respectively. SSCs can be classified into different classes according to the categories of the functions they perform or the design provisions they act as. Appropriate requirements are applied to these SSCs according to their safety class.

In a general and overall point of view, with a basic understanding of the plant design and its safety analysis, the classification of SSCs starts at the identification of safety functions and design provisions. Detailed information except those about identification of design

provisions is provided in other chapters of this PSR:

a) See Chapter 2, 5, 6, 7, 8, 9, 10, 11 and 16 for information about the design of HPR1000 (FCG3) plant, systems and structures;

b) See Chapter 12, 13, 14, 18 and 19 for information about the safety and hazard analysis of HPR1000 (FCG3);

c) See Sub-chapter 4.5 for information about safety functions of HPR1000 (FCG3).

Design provisions, however, usually refer to those components and structures whose contribution to safety isn't explicitly defined by the safety functions performed as a set of action in normal operation or during an event, but provided by its inherent characteristics during all states and conditions of the plant.

4.7.3 Categorisation and Classification Related to Safety Functions

In the categorisation of safety functions, following factors are considered to identify the importance of safety functions:

a) The consequences of failure to perform the safety function. Based on the worst consequences may be led to by the failure of the safety function, the severity of consequences is divided into three levels (high, medium and low) after being compared with specific criteria for HPR1000 (FCG3) (e.g. regulatory limits about the radiological consequences of each kind of plant conditions);

b) The frequency of the occurrence of the postulated initiating events for which the function will be called upon. For HPR1000 (FCG3), this factor can be interpreted as the category of the postulated initiating events or their consequential conditions, e.g. DBC-2/3/4 and DEC-A/B. The definitions of DBCs and DECs are described in Chapter 12 & 13 respectively;

c) The significance of the contribution of the function in achieving a particular plant state after a PIE, e.g. the function is necessary for reaching a controlled state or a safe state of DBC-2/3/4, a final state of DEC-A, or only for DEC-B mitigation. The definitions of each state are described in Chapter 12 & 13 respectively.

Considering these factors, safety functions are categorised into the following three categories:

a) Safety category 1 function (FC1):

    1) Function required to reach a controlled state in DBC2, 3 and 4 whose failure may result in 'high' consequences.

b) Safety category 2 function (FC2):

    1) Function required to reach a controlled state in DBC2, 3 and 4 whose failure may result in 'medium' consequences;

2) Function required to reach and to maintain a safe state in DBC2, 3 and 4 whose failure may result in ‘high’ consequences.

c) Safety category 3 function (FC3):

1) Function whose failure may result in ‘low’ consequences in DBC2, 3 and 4;

2) Function required to reach and to maintain a safe state in DBC2, 3 and 4 whose failure may result in ‘medium’ consequences;

3) Function required to reach and to maintain a final state of DEC-A or to mitigate DEC-B whose failure may result in ‘high’ consequences;

4) Function that prevents the actuation of the reactor trip and engineering safety systems during deviation from normal operation, including those designed to maintain the main plant parameters with in the normal range of operation of the plant;

5) Function that provides necessary monitoring information and communication means for emergency response of workers and the plant under DBC3 and 4 and DEC;

6) Function used to achieve hazard protection objectives in the hazard analysis;

7) The lowest functional categorisation of isolation function used to isolate items with different safety classes is FC3.

If a function is used under different conditions, its function categorisation depends on the condition that leads to the highest category.

The classification of functions under different conditions in HPR1000 (FCG3) is shown in T-4.7-1. ‘NC’ denotes non-categorised functions which are not included in the description above.

T-4.7-1 Function categorisation under different conditions

Type of Safety Functions	Consequence of Failure		
	High	Medium	Low
Before a controlled state under DBC2, 3 and 4 conditions	FC1	FC2	FC3
Before a safe state under DBC2, 3 and 4 conditions	FC2	FC3	FC3
Before a final state under DEC-A or mitigating DEC-B	FC3	NC	NC

The class of SSCs that fulfil specific safety functions should be consistent with the category of that safety function:

a) SSCs that fulfil safety category 1 functions (FC1) are classified as function class 1 items (F-SC1);

b) SSCs that fulfil safety category 2 functions (FC2) are classified as function class 2 items (F-SC2);

c) SSCs that fulfil safety category 3 functions (FC3) are classified as function class 3 items (F-SC3).

The function class of SSCs which are not classified into F-SC1, F-SC2 and F-SC3 are non-classified and denoted as 'NC'.

SSC classes may be lowered provided that it can be proven that SSCs have enough reliability and time to fulfil safety functions following a PIE, e.g. that SSCs have enough time to be maintained or replaced.

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

4.7.4 Categorisation and Classification Related to Design Provisions

SSCs that are designed as design provisions are classified directly according to the consequences of failure. The definition of consequences of failure is the same as the failure consequences of safety functions described in Sub-chapter 4.7.3. Similarly, consequences are divided into high, medium and low categories. The categorisation and classification are described as below:

a) Design provisions whose failure may result in 'high' consequences under DBC1 are categorised as High-consequence Design Provisions (DPH) and the SSCs act as that design provision are classified as barrier class 1 items (B-SC1);

b) Design provisions whose failure may result in 'medium' consequences under DBC1 are categorised as Medium-consequence Design Provisions (DPM) and the SSCs act as that design provision are classified as barrier class 2 items (B-SC2);

c) Design provisions whose failure may result in 'low' consequences under DBC1 are categorised as Low-consequence Design Provisions (DPL) and the SSCs act as that design provision are classified as barrier class 3 items (B-SC3);

d) Design Provisions used to achieve hazard protection objectives in the hazard analysis are categorised as Hazard-protection Design Provision (DPZ) and the SSCs act as that design provision are classified as hazard protection class 3 (Z-SC3).

All design provisions other than DPH, DPM, DPL and DPZ are categorised as Accident Design Provisions (DPA), including:

a) For pipes acting as the reactor coolant system pressure boundary whose leakage cannot be compensated by normal makeup method (e.g. one charging pump) in case of pipeline breakage, though the failure only results in 'medium' consequences (therefore should have been categorised as DPM), they are classified as B-SC1 according to engineering experience of similar pressurised water reactors;

b) For pipes and tubes acting as the reactor coolant system pressure boundary whose leakage can be compensated by normal makeup method (e.g. one charging pump) in case of pipeline breakage, they are classified as B-SC2 according to engineering

experience of similar pressurised water reactors;

c) Components (including pipes) that need to be connected to the primary loop under DBC2, 3 and 4 and DEC conditions and contain high radioactive fluid (radioactive coolant fluid contaminated after the loss of fuel cladding integrity) are classified as B-SC2;

d) SSCs whose failure may cause the containment to be bypassed under DBC2, 3 and 4 and DEC conditions are classified as B-SC2.

The barrier class of SSCs which are not classified into B-SC1, B-SC2 and B-SC3 are denoted as 'NC'.

If an SSC acts as multiple design provisions, its classification depends on the design provision which leads to the highest class of this SSC.

Generally, the barrier class won't be defined for electrical and I&C SSCs as they don't act as any design provision.

4.7.5 Design Requirements of SSCs

4.7.5.1 Design Requirements of Systems

For achieving appropriate reliability of the systems to perform safety functions, a set of design requirements of systems is defined. For the same reason, the design requirements of a system are defined mainly according to its function class.

Function design requirements directly affect the design requirements for specific SCCs that fulfil functions, especially the systems. Those 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).

Safety function and system design requirements are shown in T-4.7-2.

4.7.5.2 Design Requirements of Structures and Components

As described in Section 4.7.3 and 4.7.4, both a barrier class and a function class are defined for a component (or structure) and the design requirements of this component (or structure) are identified according to both its barrier class and its function class.

Appropriate design requirements are applied in the design of structures and components according to their safety class as described below:

F-SC1, F-SC2, B-SC1, B-SC2 and B-SC3 components and structures are designed in accordance with requirements of Chinese or international nuclear industry codes and standards. If there are no appropriate nuclear industry codes and standards, equivalent requirements may be applied.

For F-SC3 components and structures, appropriate non-nuclear codes and standards are applied, with exception to I&C equipment for which nuclear industry codes and standards exist.

More information about codes and standards applied for structures and components are provided in Sub-chapter 4.8 ‘Codes and Standards’.

T-4.7-2 System Design Requirements

Function Categorisation	System Classification	Single Failure Criterion[1]	Physical and Electrical separation	Emergency Power Supply	Periodic Test[6]	Environmental Qualification[7]	Protection Against Internal and External Hazards (Including Earthquakes)
FC1	F-SC1	Yes System level[2]	Yes	Yes	Yes	Yes	Yes
FC2	F-SC2	Yes Function level[2]	Yes[4]	Yes	Yes	Yes	Yes
FC3	F-SC3	No[3]	Special requirements[5]	Case by case	Yes	Case by case	Case by case

Note 1: Both active and passive single failures are considered when the criterion are applied, however passive single failures are considered only after 24 hours from the occurrence of PIEs.

Note 2: Considering single failure criterion at the ‘system level’ of FC1/F-SC1 indicates that these systems must be redundant. Considering single failure criterion at the ‘function level’ for systems fulfilling FC2/F-SC2 functions indicates that these systems may not need redundancy. When an FC2 system is subject to non-redundant design, another system must fulfil the same function (with functional diversity) and single failure evaluation of this function must be performed. In this case, multiple pipelines of different systems fulfilling the same function should use physical isolation requirements.

Note 3: FC3 functions generally need not follow single failure criterion. For a function required to reach and maintain a safe state under DBC-2 conditions, if its failure may result in ‘medium’ consequences, then this function needs to follow single failure criterion.

Note 4: Against redundant system or function diversity series.

Note 5: FC3/F-SC3 systems are properly zoned and isolated from FC1/F-SC1 and FC2/F-SC2 systems, especially from functions and systems at different Defence in

Depth (DiD) levels, according to analysis results of internal and external hazards.

Note 6: Active Safety systems must be designed so that periodic testing can be performed, except the case where continuous operation is required.

Note 7: Qualification requirements are determined according to the specific equipment operational environment. In particular, equipment performs FC3 functions that copes with design extension conditions should meet requirements for environmental radioactivity, pressure, temperature, etc. in a corresponding design extension conditions.

4.7.6 Seismic Requirements

Two seismic categories are defined, i.e. Seismic Category 1 (SSE1) and Seismic Category 2 (SSE2). Those that are not categorized as Seismic Category 1 and Seismic Category 2 are marked with 'NO'.

General seismic requirements are divided into four categories as follows:

a) Operability (O), it is the capability of an active component, including all necessary auxiliary, supporting and energy supply systems, to perform its intended functions and to meet the safety objective;

b) Functional capacity (F), it is the ability of all pressure-bearing parts of components to withstand the specified loadings with limited deformations such that its capacity is not impaired by a possible flow reduction;

c) Integrity (I), it is the ability of all pressure-bearing parts of components safely to withstand the specified loadings at the given frequency of occurrence throughout the service life of the component;

d) Stability (S), it is the ability of a component to withstand loads which tend to change the orientation or location of the component (e.g. toppling, falling and impermissible slip, shearing off of parts).

SSCs of Seismic Category 1 are designed to perform their safety function or act as design provisions during or after an earthquake with maintaining their operability, functional capacity, integrity or stability.

SSCs of B-SC1, B-SC2, F-SC1 and F-SC2 are designed according to the seismic requirements of Seismic Category 1.

B-SC3 components are not categorised into Seismic Category 1 if the leakage caused by the failure of their integrity can be contained by Seismic Category 1 structures.

F-SC3 components which contribute to protection and mitigation in DECs, or which used to provide fire detection and protection in building containing F-SC1, F-SC2 components are categorised as Seismic Category 1.

SSCs whose failure after an earthquake may lead to unacceptable impacts on adjacent Seismic Category 1 SSCs are categorised as Seismic Category 2. Usually, SSCs of Seismic Category 2 are required to maintain their integrity or stability.

More detailed seismic requirements of civil structures are described in Chapter 16.

4.8 Codes and Standards

This sub-chapter lists the codes and standards applied for HPR1000 (FCG3). Codes and standards are selected in accordance with the safety category of the function and safety class of the structures systems and components (SSCs) which are defined in sub-chapter 4.7. The codes and standards applied should reflect the functional reliability requirements

of the structures, systems and components, and be commensurate with their safety classification.

This sub-chapter lists codes and standard applied in the following technical areas:

a) Structural Integrity;

b) Mechanical;

c) Control and Instrumentation;

d) Electrical;

e) Civil Engineering;

f) Hazard and Fire Protection (nuclear island buildings fire only)

g) Quality Assurance.

The Requesting Party (RP) has recognised that UK nuclear safety regulations are based on a non-prescriptive regime and consequently the technical codes and standards that must be used for nuclear power plant are not prescribed. However, the codes and standards must represent relevant good practice.

The application risks of codes and standards have been identified, including version, mixing and unfamiliar codes and standards for UK regulators. To close those risk items, the analysis is undertaken. In the design of UK HPR1000, in principle, the last edition will be applied for UK HPR1000. Where it's not practicable to do so, a justification will be provided. To ensure completeness and consistency of codes and standards, mixing of codes and standards will be avoid, the special case will be demonstrated to ensure the compatibility. The appropriate international good practice will be considered in the design of UK HPR1000, such as civil engineering and construction, quality assurance etc.

The codes and standards list in this sub-chapter are applied in the design of HPR1000 (FCG3), and the list of codes and standards applied in UK HPR1000 will be completed after analysis. The requirements of UK regulators and the strategy of identified risk will be considered for principles of codes and standards used in the design of UK HPR1000.

a) Structural Integrity

The processes followed for the structural integrity assessment are discussed in detail in Chapter 17.

Table 4.8-1 identifies the major codes and standards applied for B-SC1 components and relevant supports (including all reactor vessel internals).

Table 4.8-2 identifies the major codes and standards applied for B-SC2, B-SC3, F-SC1 and F-SC2 components and relevant supports.

T-4.8-1 Applicable codes and standards for B-SC1 components and relevant supports (including all reactor vessel internals)

SSCs Type	Applicable Codes and Standards
Reactor Pressure Vessel	RCC-M-2007 Section I Subsection A RCC-M-2007 Section I Subsection B RCC-M-2007 Section I Subsection Z RCC-M-2007 Section I Subsection H (for Supports) RCC-M-2007 Section I Subsection G (for RVI) RCC-M-2007 Section II RCC-M-2007 Section III RCC-M-2007 Section IV RCC-M-2007 Section V RSE-M-2010+2012 Addendum Section I Subsection A RSE-M-2010+2012 Addendum Section I Subsection B RSE-M-2010+2012 Addendum Section II RSE-M-2010+2012 Addendum Section III 3.1.I RSE-M-2010+2012 Addendum Section III 3.2
Main coolant piping	
Pressuriser	
Pumps	
Valves	
Supports	
Reactor Vessel Internals	
Steam Generators[1]	ASME-2007, 2008a Addenda BPVC Section II ASME-2007, 2008a Addenda BPVC Section III Division 1 ASME-2007, 2008a Addenda BPVC Section V ASME-2007, 2008a Addenda BPVC Section IX ASME-2007, 2008a Addenda BPVC Section XI RSE-M-2010+2012 Addendum Section I Subsection A RSE-M-2010+2012 Addendum Section I Subsection B RSE-M-2010+2012 Addendum Section II RSE-M-2010+2012 Addendum Section III 3.1.I RSE-M-2010+2012 Addendum Section III 3.2

Note 1: For the steam generator, the ASME Code has been selected as the code of design, fabrication, inspection and testing. Pre-service and in-service Inspection of the Steam Generator is performed according to RSE-M.

T-4.8-2 Applicable codes and standards for B-SC2, B-SC3, F-SC1 and F-SC2 components and relevant supports

SSCs Type	Applicable Codes and Standards
Pressure Vessels	RCC-M-2007 Section I Subsection A RCC-M-2007 Section I Subsection Z RCC-M-2007 Section I Subsection C RCC-M-2007 Section I Subsection D RCC-M-2007 Section I Subsection H (for supports)
Heat Exchangers	
Piping	

SSCs Type	Applicable Codes and Standards
Pumps	RCC-M-2007 Section II RCC-M-2007 Section III RCC-M-2007 Section IV RCC-M-2007 Section V RSE-M-2010+2012 Addendum Section I Subsection A RSE-M-2010+2012 Addendum Section I Subsection C RSE-M-2010+2012 Addendum Section I Subsection D RSE-M-2010+2012 Addendum Section II RSE-M-2010+2012 Addendum Section III 3.1.II RSE-M-2010+2012 Addendum Section III 3.2
Valves	
Supports	

b) Mechanical

T-4.8-3 identifies the major codes and standards applied in the design of mechanical components.

T-4.8-3 Mechanical Codes and Standards

SSCs Type	Applicable Codes and Standards
Safety Classified Pressure Retaining Mechanical Equipment	RCC-M-2007 ASME (selected for SG)
HVAC	NB/T 20038-2011 Code on Nuclear Air and Gas Treatment-General Requirements on Design and Fabrication
Handling Equipment	GB/T 3811-2008 Design Rules for Cranes

c) Control and Instrumentation

T-4.8-4 identifies the major codes and standards applied in the design of Control and Instrumentation.

T-4.8-4 C&I Codes and Standards

Codes and Standards	Title
IEC 61513-2011	Instrumentation and control systems important to safety – General requirement
IEC 60880-2006	Nuclear power plants – Instrumentation and control important to safety – software aspects for computer-based systems performing category A functions
IEC 62138-2004	Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B and C functions
IEC 60780-1998	Nuclear power plants - Electrical equipment of safety system –

Codes and Standards	Title
	Qualification
IEC 60980-1989	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear
IEEE 603-2009	Standard Criteria for Safety Systems for Nuclear Power Generating Stations

d) Electrical code

T-4.8-5 identifies the major electrical codes and standards.

T-4.8-5 Electrical Codes and Standards

Codes and Standards	Title
GB/T 12788-2008	Criteria for class 1E power systems for nuclear power generating stations
GB/T 13626-2008	Application of the single failure criterion to safety systems in nuclear power plant
GB/T 13177-2008	Preferred power supply for nuclear power plants
GB/T 13284-2008	The safety systems for nuclear power plants-Part 1: Design criteria
EJ/T 625-2004	Criteria for diesel-generator units applied as standby power supplies for nuclear power generating stations
NB/T 20066-2012	The design criteria for nuclear power plants station blackout

e) Civil Engineering

T-4.8-6 identifies the major codes and standards applied in the design of civil engineering.

T-4.8-6 Civil Engineering Codes and Standards

Codes and Standards	Title
NB/T 20303-2014	Design Requirements for Prestressed Concrete Containment for Pressurized Water Reactor Nuclear Power Plants
NB/T 20012-2010	Design Requirements for Nuclear Safety Related Concrete Containments for Pressurized Water Reactor Nuclear Power Plant
NB/T 20011-2010	Design Requirements for Nuclear Safety Related Steel Structure for Pressurized Water Reactor Nuclear Power Plant
NB/T 20105-2012	Load code for the design of nuclear power plants building structures
GB 50267-1997	Code for seismic design of nuclear power plant
GB 50011-2010	Code for seismic design of buildings

f) Hazard and Fire Protection (nuclear island building fire only)

T-4.8-7 identifies the major codes and standards applied in the area of fire protection.

T-4.8-7 Hazard and Fire Protection Codes and Standards

Codes and Standards	Title
ETC-F-2010	EPR Technical Code for Fire Protection
NS-G-1.11-2004	Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants

g) Quality Assurance

The quality assurance management processes are discussed in detail in Chapter 20.

T-4.8-8 identifies the major codes and standards applied in the area of quality assurance.

T-4.8-8 Quality Assurance Codes and Standards

Codes and Standards	Title
HAF 003-1991	Quality Assurance for Safety in Nuclear Power Plant
ISO 9001-2008	Quality management systems-Requirements

4.9 Equipment Qualification

Equipment qualification is the procedure of the generation and maintenance of evidence to ensure that equipment will operate on demand to meet system performance requirements. Equipment qualification includes environmental and seismic qualification.

The main methods for qualification include type test, analysis method and combined method.

This section shows for HPR1000 (FCG3) that qualification procedures have been applied which confirm that all SSCs will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety cases such as ambient conditions (P,T, humidity, radiations), internal conditions (for fluid systems: debris source term), and for the duration of their operational lives.

It has been noticed that the qualification procedures has been recommended by the SAP EQU.1. There is no difference between the claim of the SAP EQU.1 and HPR1000 (FCG3).

4.9.1 Equipment to Be Qualified

Equipment qualification is intended to produce and maintain evidence to support claims that equipment should fulfil their allocated safety functions.

In combination with safety classification requirements for equipment, the specific equipment to be qualified is as follows:

a) Active mechanical equipment and electrical equipment that perform FC1 or FC2 function;

b) Active mechanical equipment and electrical equipment that perform FC3 function, including:

   1) Functions required to maintain a safe state;

   2) Any functions which can mitigate the DEC condition, whose failure may lead to ‘high’ consequences.

c) Equipment whose seismic requirement is Operability (O), integrity (I) or stability (S) but they do not perform above functions. This equipment requires seismic qualification.

4.9.2 Qualification Category

To distinguish the equipment to be qualified, the equipment is sorted into several categories upon the locations and the safety functions of equipment.

Category K1 equipment: Equipment installed inside the containment, capable of functioning under environmental conditions corresponding to normal, accidental and/or post-accidental plant operating conditions and under seismic load.

Category K2 equipment: Equipment installed inside the containment, capable of functioning under environmental conditions corresponding to normal plant operating conditions and under seismic load.

Category K3 equipment: Equipment installed outside the containment, capable of functioning under environmental conditions corresponding to normal plant operating conditions and under seismic load.

Category K3ad equipment: Equipment installed outside the containment, capable of functioning under environmental conditions corresponding to normal, accidental and/or post-accidental plant operating conditions and under seismic load.

Category SA equipment: Equipment installed inside or outside the containment, capable of functioning under environmental conditions corresponding to severe accidental and/or post- severe accidental plant operating conditions and under seismic load.

4.9.3 Qualification Methods

Generally qualification methods include type test, analysis method and combined method. Meanwhile, the internal conditions of equipment are considered during the qualification process.

4.9.3.1 Type Test

Type tests are tests where the various conditions of the nuclear power plant are simulated by using test units to verify whether the equipment function can be fulfilled. This then

justifies the use of the remainder of the group of components.

If this method is adopted, the load identical to that under operating conditions will be imposed on the equipment. The equipment used in the test shall fully representative of the actual equipment that will operate in the plant. Each qualification test shall be carried out separately and in the order of the most representative operating conditions the equipment will undergo or the load the equipment will bear.

When type tests are used in equipment qualification, the applicable standards and practices include:

a) International standards based on IEC (such as IEC60780);

b) French practices based on French standard and relevant specifications;

c) American practices based on IEEE Standard and ASME Code as well as other relevant specifications;

d) Chinese practices based on Chinese standard and relevant specifications.

For specific equipment, the qualification procedure will be in accordance with one of the above practices and all procedures stated in the practice shall be completed in the initial qualification. In other words, the qualification procedures in different qualification practices shall not be mixed.

The basic principle of qualification by testing is that any qualification test must be carried out in accordance with the qualification practice selected initially. Otherwise, documentary evidences must be provided. For example, in the process of the qualification test, if both RCC-E test items and IEEE test items are referred to, the test will be regarded as using two different methods. This qualification method is unacceptable in principle unless there is special research proving that the qualification process is reasonable.

4.9.3.2 Analysis Method

a) Calculation

The calculation method is that the equipment function is assessed by means of theory and calculation through mature analysis models and design inputs. Generally calculation method is applicable to the structural load analysis and the mechanical analysis of the equipment.

This method is usually used if:

1) The load has been estimated sufficiently and conservatively;

2) The calculation models are representative;

3) The calculation methods or codes used are valid.

Moreover, for certain equipment which cannot be qualified by testing easily, such as equipment that is large, heavy or with high operating parameters, it is acceptable to use

the calculation method for qualification on the premise to demonstrate that the above principles are satisfied.

b) Operating experience method

The operating experience method means that the safety functions of the equipment are validated by analysing the historical data of the representative equipment in power plant operation. Generally the operating experience method shall meet the following conditions:

1) The operated equipment shall be identical to or sufficiently representative of the equipment which is to be qualified;

2) The operating time shall be over a sufficiently long period;

3) The operated equipment service conditions shall be at least as harsh as HPR1000 (FCG3) conditions;

4) The documentation accompanying the operating experience shall be sufficiently accurate and detailed to justify the performance of the operated equipment.

Practically, this method is rarely used alone. It is usually used to confirm the performance of certain components of the equipment.

c) Analogy method

The analogy method which obtains qualification results by comparing the equipment to be qualified with similar equipment (called mother equipment).

The analogy method generally includes the following three steps:

1) Comparing the design structure of equipment to be qualified with the mother equipment;

2) Comparing the function and service condition of equipment to be qualified with the mother equipment;

3) Evaluating and estimating every potential failure at the equipment design stage.

4.9.3.3 Combined Method

The above equipment qualification methods can be used in combination. The principles of the combined method are subject to the equipment to be qualified. Each qualification item in the combination shall abide by the same environmental condition and all methods in the combination shall jointly prove that the equipment is capable of fulfilling its safety functions.

4.10 Design for Reliability of Structures, Systems and Components

The achievement of the safety objectives above depends on a set of items (i.e. structures, systems and components). The following design measures may be used, if necessary in

combination, to achieve and maintain the necessary reliability of these items commensurate with their safety significance.

It has been noticed that in SAPs, EDR.1~EDR.4 and relevant contents also present the aspects which should be considered for reliability of SSCs. There may be several gaps or differences between the reliability requirements applied for HPR1000 (FCG3) and those recommended in SAPs and it will be addressed appropriately for UK HPR1000 and demonstrated in PCSR.

a) Single failure criterion

According to IAEA Safety Standards No.SSR-2/1 in Reference [2], a single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system who perform safety function(s), 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:

1) An active single failure is defined as a failure which is sufficient to prevent the relevant safety function of a component, including the malfunction of a mechanical or electrical component which relies on mechanical movement to complete its intended function upon demand, and the malfunction of an I&C component;

2) A passive single failure is defined as a failure, which can occur in a component that does not need to change its state in order to carry out its function. The passive single failure is considered 24 hours after the occurrence of the postulated initiating event.

More than the minimum number of components is provided to carry out any safety function to ensure the single failure criterion (SFC) is implemented.

In the design of HPR1000 (FCG3), the single failure criterion is applied to systems which perform the FC1 or FC2 functions, so that a sufficient degree of redundancy is ensured in the design of these systems.

There are several differences in detailed application of the Single Failure Criterion between the design of HPR1000 (FCG3) and UK regulatory expectations. For example, it is clear that the Single Failure Criterion applies to ensure the performance of safety functions in SAP EDR.4. In the design of HPR1000 (FCG3), the Single Failure Criterion is applied to ‘systems level’ and ‘function level’ for systems which perform FC1 and FC2 functions respectively. However, it should be noted that the design principles applied for HPR1000 (FCG3) is based on the international good practice. The differences between HPR1000 (FCG3) and UK regulatory expectations will be appropriately addressed for UK HPR1000 and the compliance with UK regulatory expectations will be demonstrated in PCSR of UK HPR1000.

b) Independence

The following principles for independence are applied in the design:

1) Independence between the trains of redundant system components are maintained as far as reasonably practicable;

2) Independence between the items of highest safety class and others are maintained as far as reasonably practicable;

3) Independence between the items of different safety categories as far as reasonably practicable to avoid the effects on a higher safety category item from a lower one;

4) The components designed to mitigate a potential initiating event are independent with the effects of this potential initiating event as far as reasonably practicable.

Independence could be accomplished in the design of systems by using functional isolation and/or physical separation.

c) Diversity

Diversity is applied in redundant systems or component to achieve the reliability target incorporating different attributes to perform the same safety function. The attributes can be referred to different operating conditions, different manufacturers, different physical variables, or different principles of operation, etc.

In HPR1000 (FCG3), some safety features are designed to be diverse to elevate the overall probabilistic safety level of plant in the consideration of Common Cause Failure (CCF). Most of these features are called DEC-A features that mitigate the DEC-A sequences. DEC-A sequences are complex sequences with multiple failures (including Common Cause Failure). Further information about DEC-A sequences and DEC-A features are provided in Chapter 13.

It is noticed that a strong emphasis in the UK context on the implementation of diversity between main lines and diverse line of defence for frequent faults. Notably, diversity provisions to be implemented between the lines of defence identified in the Fault Schedule (first line/diverse line for frequent faults) is very important in order to ensure that a Common Cause Failure affecting the first line of protection cannot prevent the diverse line of protection to perform its function in the frame of a given initiating event.

The implementation of diversity recommended by SAPs is not exactly the same as that of HPR1000 (FCG3). The gap has already been identified and it will be appropriately addressed in PCSR.

d) Fail-safe

The fail-safe requirement are considered and incorporated, as appropriate, into the design of systems and components of HPR1000 (FCG3), so that their failure or the failure of a

support feature does not prevent the performance of the intended safety function. For example, the safety function is to remain closed to play a segregated role for many valves. These valves would be closed automatically when they lose power.

According to SAP EDR.1, due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate.

There are some differences about description between the fail-safe principle in SAPs and those of HPR1000 (FCG3). These differences will be considered appropriately for UK HPR1000.

4.11 References

[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, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, No.SSG-30, May 2014.

[4] IAEA, Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA-TECDOC-1787, April 2016.

[5] ONR, Categorisation of Safety Functions and Classification of Structures, Systems and Components, NS-TAST-GD-094, Revision 0, November 2015.