



<b>UK EPR</b>	Title: PCSR – Sub-chapter 3.2 – Classification of structures, equipment and systems	
	<b>UKEPR-0002-032 Issue 04</b>	
	Total number of pages: 74	Page No.: I / IV
Chapter Pilot: M. BERNARD		
Name/Initials  Date 15-11-2012		
Approved for EDF by: A. MARECHAL	Approved for AREVA by: G. CRAIG	
Name/Initials <i>A. Se. Maehal</i> Date 16-11-2012	Name/Initials  Date 16-11-2012	

### REVISION HISTORY

Issue	Description	Date
00	First issue for INSA information	04.01.08
01	Integration of technical and co-applicant review comments	29.04.08
02	PCSR June 2009 update: <ul style="list-style-type: none"> <li>- Integration of references</li> <li>- Clarification of text</li> </ul>	25.06.09
03	Consolidated Step 4 PCSR update: <ul style="list-style-type: none"> <li>- Minor editorial changes</li> <li>- Full rewrite of the sub-chapter, in accordance with the updated UK EPR classification scheme (use of Category A, B, C and Class 1, 2, 3) and with the design change proposed for UK EPR I&amp;C architecture, and to consistently apply the methodology to Civil Structures; plus further details in some sub-sections (3.2.2, 3.2.3, 5.2, 6.1.1, 6.1.2)</li> <li>- Inclusion of High Integrity Components (HIC) under M1 requirements (§6.3.3.1)</li> <li>- Update to classification of CRDM (Table 1)</li> </ul>	31.03.11
04	Consolidated GDA PCSR update: <ul style="list-style-type: none"> <li>- References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc</li> <li>- Full rewrite of the sub-chapter, in accordance with the updated UK EPR classification: new definitions for SSC, SFG, SF; addition of references; new section covering ALARP; definition of LLSF in relation to the level of defence in depth; category A, B and C criteria fully consistent with IEC 61226; section 4 completed and clarified; section 5 restructured to define architecture requirements; addition of a new summary table; new section 6 added to define system requirements; section 7 restructured to define components requirements; addition of a new summary table; new section 8 for civil structures and section 9 for PSA review.</li> </ul>	16-11-12

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 3.2 – Classification of structures, equipment and systems	
	<b>UKEPR-0002-032 Issue 04</b>	Page No.: II / IV

**Copyright © 2012**

**AREVA NP & EDF  
All Rights Reserved**

This document has been prepared by or on behalf of AREVA NP and EDF SA in connection with their request for generic design assessment of the EPR™ design by the UK nuclear regulatory authorities. This document is the property of AREVA NP and EDF SA.

Although due care has been taken in compiling the content of this document, neither AREVA NP, EDF SA nor any of their respective affiliates accept any reliability in respect to any errors, omissions or inaccuracies contained or referred to in it.

All intellectual property rights in the content of this document are owned by AREVA NP, EDF SA, their respective affiliates and their respective licensors. You are permitted to download and print content from this document solely for your own internal purposes and/or personal use. The document content must not be copied or reproduced, used or otherwise dealt with for any other reason. You are not entitled to modify or redistribute the content of this document without the express written permission of AREVA NP and EDF SA. This document and any copies that have been made of it must be returned to AREVA NP or EDF SA on their request.

Trade marks, logos and brand names used in this document are owned by AREVA NP, EDF SA, their respective affiliates or other licensors. No rights are granted to use any of them without the prior written permission of the owner.

#### **Trade Mark**

EPR™ is an AREVA Trade Mark.

#### **For information address:**



AREVA NP SAS  
Tour AREVA  
92084 Paris La Défense Cedex  
France



EDF  
Division Ingénierie Nucléaire  
Centre National d'Équipement Nucléaire  
165-173, avenue Pierre Brossolette  
BP900  
92542 Montrouge  
France

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 3.2 – Classification of structures, equipment and systems	
	<b>UKEPR-0002-032 Issue 04</b>	Page No.: III / IV

## TABLE OF CONTENTS

- 1. PURPOSE OF CLASSIFICATION – APPROACH FOLLOWED**
- 2. OVERVIEW OF THE CLASSIFICATION METHODOLOGY**
  - 2.1. DEFINITIONS**
  - 2.2. BACKGROUND**
  - 2.3. OVERVIEW OF UK EPR CLASSIFICATION**
  - 2.4. ALARP PRINCIPLES AND CLASSIFICATION**
- 3. SAFETY FUNCTION DEFINITION AND CATEGORISATION**
  - 3.1. DERIVATION OF SAFETY FUNCTIONS**
  - 3.2. DEFINITION OF PLANT LEVEL SAFETY FUNCTIONS (PLSF)**
  - 3.3. DEFINITION OF LOWER LEVEL SAFETY FUNCTIONS (LLSF)**
  - 3.4. LOWER LEVEL SAFETY FUNCTION CATEGORISATION**
  - 3.5. SAFETY FUNCTION CATEGORIES AND LLSF TYPES**
- 4. CLASSIFICATION**
  - 4.1. IDENTIFICATION AND CLASSIFICATION OF SAFETY FEATURE GROUPS, SYSTEMS, SAFETY FEATURES AND COMPONENTS**
  - 4.2. BOUNDARIES AND INTERFACES**
  - 4.3. SAFETY CLASSES APPLIED TO SAFETY FEATURE GROUPS, SAFETY FEATURES AND COMPONENTS**
  - 4.4. SAFETY CLASSES APPLIED TO SYSTEMS**
- 5. ARCHITECTURE REQUIREMENTS APPLIED TO SAFETY FEATURE GROUPS**
  - 5.1. DEFINITION OF THE ARCHITECTURE REQUIREMENTS**
  - 5.2. ARCHITECTURE REQUIREMENTS PER LINE OF DEFENCE**
  - 5.3. SUMMARY OF ARCHITECTURE REQUIREMENTS PER LINE OF DEFENCE**
  - 5.4. ARCHITECTURE REQUIREMENTS BETWEEN LINES OF DEFENCE**

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 3.2 – Classification of structures, equipment and systems	
	<b>UKEPR-0002-032 Issue 04</b>	Page No.: IV / IV

- 6. REQUIREMENTS APPLIED TO SYSTEMS**
- 7. REQUIREMENTS APPLIED TO COMPONENTS**
  - 7.1. ROBUSTNESS AGAINST EARTHQUAKE**
  - 7.2. ROBUSTNESS AGAINST LOOP**
  - 7.3. QUALIFICATION FOR ACCIDENT CONDITIONS**
  - 7.4. COMPONENT REQUIREMENTS**
  - 7.5. SUMMARY OF COMPONENT REQUIREMENTS**
- 8. CLASSIFICATION AND REQUIREMENTS APPLIED TO STRUCTURES**
  - 8.1. ROLE OF STRUCTURES AND SAFETY FUNCTIONS**
  - 8.2. SAFETY CLASSES APPLIED TO STRUCTURES**
  - 8.3. STRUCTURE REQUIREMENTS**
  - 8.4. SUMMARY OF SAFETY CLASSES AND REQUIREMENTS**
- 9. CLASSIFICATION AND PSA FEEDBACK**
- 10. APPLICATION OF UK EPR CLASSIFICATION APPROACH**

## **SUB-CHAPTER 3.2 – CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS**

### **1. PURPOSE OF CLASSIFICATION – APPROACH FOLLOWED**

The safety of the plant is dependent on the performance of its Structures, Systems and Components (SSCs) in normal, hazard and fault conditions. The effect on nuclear safety of the failure of a structure, system or component depends on its significance and role.

The main purpose of a classification scheme is to help ensure that the plant is designed, manufactured, constructed, commissioned and operated so that the appropriate level of reliability and integrity is achieved for its SSCs.

The classification process involves the systematic assessment of the importance to nuclear safety of each component and its allocation to a safety class on the basis of this safety significance. The safety class allocated to a component defines the design, testing and maintenance measures to be applied in its design, construction, commissioning, and operation.

The classification approach presented in this sub-chapter has been adapted from UK and other recognised international guidance and represents a 'functional' approach to classification. This approach has been developed under the Classification of SSC [Ref-1]. The steps in the classification approach can be summarised as follows:

1. Identify safety functions and assign categories based on their importance to safety.
2. Identify the Safety Feature Groups (SFGs), Systems and Safety Features (SFs) which fulfil the safety functions, and assign a classification based on the importance of the safety functions they perform.
3. Link the classification to a set of requirements for design, construction and operation, which will ensure that the components that perform or contribute to the safety functions expected are at the required level of quality.

The consequences of the classification approach are far-reaching and extend to operational requirements, e.g. in-service inspection, periodic testing, etc.

The structure of the sub-chapter is as follows:

Section 2 provides the definitions, the main international and UK guidelines that form the basis of the classification approach and an overview of the classification process.

Section 3 describes the first step of the methodology, explains the types of safety functions, and how they are categorised.

Section 4 defines the classification approach applied to safety feature groups, and safety features. The section also explains in detail the criteria for assigning safety class to a safety feature group and a safety feature and finally to every component.

Section 5 defines the architecture requirements that apply at the level of the safety feature groups and the safety features.

Section 6 defines the architecture requirements that apply at the level of systems.

Section 7 explains how the safety classification is linked to design requirements for the components. The different types of requirements are defined and an explanation is given of how they are applied.

Section 8 defines the role of the structures, the criteria for assigning safety classification and the associated requirements.

Section 9 explains the methodology for PSA review of classification.

## 2. OVERVIEW OF THE CLASSIFICATION METHODOLOGY

### 2.1. DEFINITIONS

The classification methodology uses a number of definitions, which are essential for presenting UK EPR classification methodology. The definitions are listed below:

Accident	Accident refers to PCC-3 and PCC-4 events or RRC sequences.
Anticipated Operating Occurrence (AOO)	<p><i>“An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions”</i> (IAEA Safety Glossary, 2007 Edition [Ref-1])</p> <p>AOO can be referred as PCC-2 events.</p>
Controlled State / Non-hazardous stable state	<p><i>“[The] state of the plant, where stabilisation of any transient has been achieved, the reactor is sub-critical, adequate heat removal is ensured and radioactive releases are limited.”</i> (IEC 61226 [Ref-4])</p> <p>A controlled state is considered to be a non-hazardous stable state in the analysis of PCC-2 to PCC-4 plant events.</p>
Confinement / Containment	<p><i>“Prevention or control of releases of radioactive material to the environment in operation or in accidents.”</i></p> <p><i>“Confinement is closely related in meaning to containment, but confinement is typically used to refer to the safety function of preventing the ‘escape’ of radioactive material, whereas containment refers to the means for achieving that function.”</i> (IAEA Safety Glossary, [Ref-1])</p> <p>Confinement is used within the functional approach of this sub-chapter.</p>
Component	See Structures, Systems and Components
Design Basis Event / Design Basis Sequence	A design basis event is a Postulated Initiating Event that may occur. It relates to PCC and hazards events. Design Basis Sequences are fault sequence involving postulated failures.

Diverse line of protection functions	See Line of defence in depth.
Duty system	These systems are part of the Safety Related Systems (SRSs). The “duty” systems represent the normal operational equipment used within a NPP. They are often systems whose prime function is not safety related but failure could threaten safety by placing a demand on a safety class 1 system.
Final State / Non-hazardous stable state	For the RRC-A and the functional diversity analysis, a final state can be defined as, the core is sub-critical, the decay heat is removed by primary or secondary systems, and the activity releases remain tolerable, consistent with the objectives of these safety analyses.  A final state is considered to be a non-hazardous stable state in the analysis of RRC-A events and the functional diversity.
First line of protection function	See Line of defence in depth.
Front-line safety feature	The main safety feature performing a Lower Level Safety Function, (In contrast to the safety features performing support functions for this Lower Level Safety Function. (IAEA DS367 [Ref-2])
Function (Safety Function)	“[A] <i>specific purpose or objective to be accomplished, that can be specified or described without reference to the technical means of achieving it</i> ”. (IEC 61226 [Ref-4])
Fundamental Safety Function	See Main Safety Function
Line of defence in depth	I&C definition from Safety principles applied to the UK EPR I&C architecture [Ref-5]: Set of systems that work together in order to prevent escalation from anticipated operational occurrence to accident conditions or to stop the accident progression and bring the plant to a non-hazardous stable state.  Several lines of defence in depth are defined in the safety principles [Ref-5] in accordance with SAP EKP.3 [Ref-6]: <ul style="list-style-type: none"> <li>• Preventive line of defence in depth <ul style="list-style-type: none"> <li>○ operational functions</li> <li>○ preventive safety functions</li> </ul> </li> <li>• Main line of defence in depth required to be composed of: <ul style="list-style-type: none"> <li>○ a first line of protection and</li> <li>○ a diverse line of protection for frequent postulated initiating events</li> </ul> </li> <li>• Risk reduction line of defence in depth composed of: <ul style="list-style-type: none"> <li>○ a back-up line</li> <li>○ a severe accident line</li> </ul> </li> </ul>
Lower Level Safety Functions	Safety Functions decomposed from a Plant Level Safety Function with a level of defence in depth. (IAEA DS367 [Ref-2])
Main line of defence	See Line of defence in depth

Main Safety Function	One of the three high level safety functions: Control of fuel reactivity, Fuel heat removal, Confinement (also known as Fundamental safety function)
Non-hazardous stable state	<p><i>“State of the plant, where stabilisation of any transient has been achieved, the reactor is subcritical, adequate heat removal is ensured and radioactive releases are limited.</i></p> <p><i>Note - A transient is considered to be stabilised when, for all safety significant parameters, the margins (e.g. between the heat removal capacity and heat generation) are either stable or increasing, or sufficient margin remains to cover all expected physical processes.”</i> (IEC 61226 [Ref-4])</p> <p>It encompasses both the controlled (PCC-2 to PCC-4 events) and the final (RRC events and functional diversity analysis) states.</p>
Normal Operation	The operating condition in which the plant parameters are within normal range (i.e. PCC-1, no PCC-2 to PCC-4 or RRC event has been initiated).
Operating Conditions	The condition in which the plant is operating under normal and faulted conditions (PCC, RRC, Hazards) considered in the safety analysis and for which a safe shutdown state must be reached (e.g. Controlled and Safe shutdown states for PCC analyses, Final state for RRC-A sequences, ...).
Operational functions	See Line of defence in depth.
Physical separation	<p>Separation by geometry (distance, orientation, etc) or by appropriate barriers or by a combination thereof. (Safety principles applied to the UK EPR I&amp;C architecture [Ref- 5])</p> <p>This definition corresponds to <i>“segregation”</i> in HSE SAPs [Ref-6]</p>
Plant Level Safety Functions	Safety Functions derived from the Main Safety Functions, on the highest level. Plant level safety functions are defined independently of the operating condition. (IAEA DS367 [Ref-2])
Postulated Initiating Event (PIE)	<i>“An event identified during the design as capable of leading to an anticipated operational occurrences [AOO] or accident conditions”</i> (IAEA Safety Glossary [Ref-1])
Preventive Safety Functions	See Line of defence in depth.
Risk reduction functions	See Line of defence in depth.
Safety	<i>“In this document, ‘safety’ refers to the safety of persons in relation to radiological hazards.”</i> SAPs [Ref-6]
Safe shutdown state	State reached after the controlled state is achieved, where the core is subcritical, residual heat removal is established on a long-term basis, and radioactive discharges remain acceptable.
Safety Category	<p>A reflection of the safety significance of the Lower Level Safety Functions in terms of predefined categorisation rules.</p> <p>The terms ‘category’ and ‘class’ are sometimes used as synonyms. For the purpose of clarity in this sub-chapter, the term ‘category’ is reserved for the safety functions and the term ‘class’ for the SFG/SF, electrical and I&amp;C systems and components.</p>
Safety Class	A reflection of the safety significance of an SFG, an SF, a system or a component in terms of predefined classification rules.



Safety Feature (Sub-system)	Group of components generally belonging to a single system and working together to achieve a single action which is part of an SFG. They are in essence mechanical features, I&C instrumentation features, I&C automation features and electrical features.
Safety Feature Group	All the components that must work together to perform a Lower Level Safety Function. This will include the Front line and Support components and associated I&C actuation. A Safety Feature Group is composed of one or several Safety Features. Derived from: <i>“All the SSCs required to perform a ‘function important to safety’ should be identified and grouped into ‘feature groups’<sup>1</sup>. Depending on the design, a particular SSC can be allocated to more than one function, and thus could be assigned to several feature groups.”</i> (IAEA DS367 [Ref-2])
Single Failure Criterion (SFC)	<i>“A single failure is a failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it.</i> <i>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.”</i> (IAEA Safety Glossary [Ref-1]) Based on this, UK EPR SFC is defined as detailed in Sub-chapter 3.1.
Structures, Systems and Components (SSC)	A physical means of fulfilling a function, encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human actions. <i>“Structures are the passive elements [generally corresponding to the civil structures]: buildings, vessels, shielding, etc.</i> <i>A system comprises several components, assembled in such a way to perform a specific (active) function.</i> <i>A component is a discrete element of a system. Examples of components are wires, transistors, integrated circuits, motors, relays, solenoids, pipework, fittings, pumps, tanks and valves.”</i> (IAEA Safety Glossary [Ref-1]) In this document a system in this context is a safety feature (see definition above), a component is a mechanical, electrical or I&C element identified to perform a function, generally a component is a motor, a sensor, a pipe, a pump, a tank, a valve, a switchboard, an I&C device.
Support components / Support Safety Feature	Components (such as component cooling, lubrication, as well as energy supply) belonging to a supporting Safety Feature, which support a front-line Safety Feature to fulfil its safety functions.

<sup>1</sup> All the SSCs working together to perform one function are in one safety feature group. All the safety feature groups that work together to mitigate the consequences of a particular postulated initiating event form a ‘safety group’ (see the IAEA Safety Glossary, 2007 edition).

System	<p>In this document this generally refers to the ECS code, which is a unique 3-letter code assigned to each system (e.g. the reactor coolant system is the RCP [RCS]) but this can also refer to:</p> <ul style="list-style-type: none"> <li>○ the general term of system used in IAEA documents and other standards, when quoted text is taken from a reference,</li> <li>○ a safety feature (see above), when explaining this term.</li> </ul>
--------	--

## 2.2. BACKGROUND

The UK EPR classification methodology is based on meeting the objectives of the HSE Safety Assessment Principles (SAPs) [Ref-4], IAEA requirements NS-R-1 [Ref-1], IAEA guidelines DS367 [Ref-2] and consideration of IEC 61226 [Ref-3]. A brief description of these texts is reproduced here.

### 2.2.1. Safety Assessment Principles

The ONR uses the Safety Assessment Principles (SAPs) [Ref-1], together with the supporting Technical Assessment Guides (TAGs), to guide regulatory decision making in the UK nuclear licensing process.

The SAPs provide ONR inspectors with a framework for making consistent regulatory judgments on nuclear safety cases. The principles are supported by TAGs and other guidance. The SAPs also provide current and prospective nuclear site licensees with information on the regulatory principles against which their safety submissions will be judged. However, the SAPs are not intended as design or operational standards, reflecting the non-prescriptive nature of the UK nuclear regulatory system.

The SAPs state that: *“The safety functions to be delivered within the [nuclear] facility, both during normal operation and in the event of a fault or accidents, should be categorised based on their significance to safety”* as follows:

A safety categorisation scheme could be determined on the following basis:

- a) *“Category A – any function that plays a principal role in ensuring nuclear safety.*
- b) *Category B – any function that makes a significant contribution to nuclear safety.*
- c) *Category C – any other safety function “*

It is further suggested that the methodology for applying this scheme should consider the following points:

- *“the consequence of failing to deliver the safety function;*
- *the extent to which the function is required, either directly or indirectly, to prevent, protect against, or mitigate the consequences of initiating faults;*
- *the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;*
- *the likelihood that the function will be called upon.*

*The categorisation of safety functions should take no account of any redundancy, diversity or independence within the design - these aspects relate to the SSCs required to deliver the safety function.”*

The categorisation assigned to each safety function should be used to classify the SSCs required to deliver that safety function.

### **2.2.2. IAEA Standards – NS-R-1 and DS367**

IAEA safety standard series NS-R-1 [Ref-1] establishes the principle of classification of NPP SSCs according to their importance to safety.

The main requirements for this classification process are summarised below:

- *“All SSCs, including software for instrumentation and control (I&C), that are important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety.*

*They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.*

- *The method for classifying the safety significance of a SSC shall primarily be based on deterministic methods, complemented where appropriate, by probabilistic methods and engineering judgement, with account taken of factors such as:*
  1. *the safety function(s) to be performed by the item;*
  2. *the consequences of failure to perform its function;*
  3. *the probability that the item will be called upon to perform a safety function;*
  4. *the time after a postulated initiating event at which, or the period throughout which, it will be called upon to operate.*
- *Appropriately designed interfaces shall be provided between SSCs of different classes to ensure that any failure in an SSC in a lower safety class will not propagate to a system classified in a higher class.”*

The IAEA Safety Guide DS367 [Ref-2] provides guidance on how to meet the requirements for identification of safety functions and classification of SSCs established in IAEA Safety Requirements NS-R-1 [Ref-1] and in particular how to ensure appropriate quality and reliability of SSCs. The process applied to UK EPR SSCs classification follows the main proposals in this sub-chapter.

### **2.2.3. IEC Standards – IEC 61226 and IEC 61513**

IEC 61226 [Ref-1] has been adopted as a British Standard and builds on the requirements established in NS-R-1 to provide guidance on the categorisation of functions according to the importance to safety of these functions. Although IEC 61226 [Ref-1] concerns the categorisation of I&C functions, the methodologies it suggests are applicable to other areas.

IEC 61226 [Ref-1] extends the categorisation strategy discussed in section 2.2.2 and establishes the criteria and methods to be used to assign the functions of an NPP into three levels reflecting the importance to safety (A, B and C). A non-classified category is used for functions with no significant safety role.

IEC 61226 [Ref-1] accepts that the national application of the principles and criteria may assign differing nomenclature to categories A, B and C but states that the principles, criteria and associated requirements should be upheld.

IEC 61513 [Ref-2] provides the link between the categorisation of functions, and the classification of I&C systems (instrumentation and control systems and equipment) which perform them.

### **2.3. OVERVIEW OF UK EPR CLASSIFICATION**

The purpose of a classification methodology is to ensure that the SSCs are systematically designed, constructed, and operated so as to fulfil the safety functions they perform and, ultimately, the fundamental safety functions, with an appropriate level of quality.

The classification process provides a structured, clear and logical method to identify the necessary safety requirements for all SSCs important to safety. This allows the identification of appropriate design solutions to fulfil the fundamental safety functions, and also provides confidence to the plant operator and the regulatory bodies that the standard of design and construction is of sufficient quality.

This section describes the overall UK EPR methodology for categorising functions and classifying SSCs in line with the applied standards discussed above.

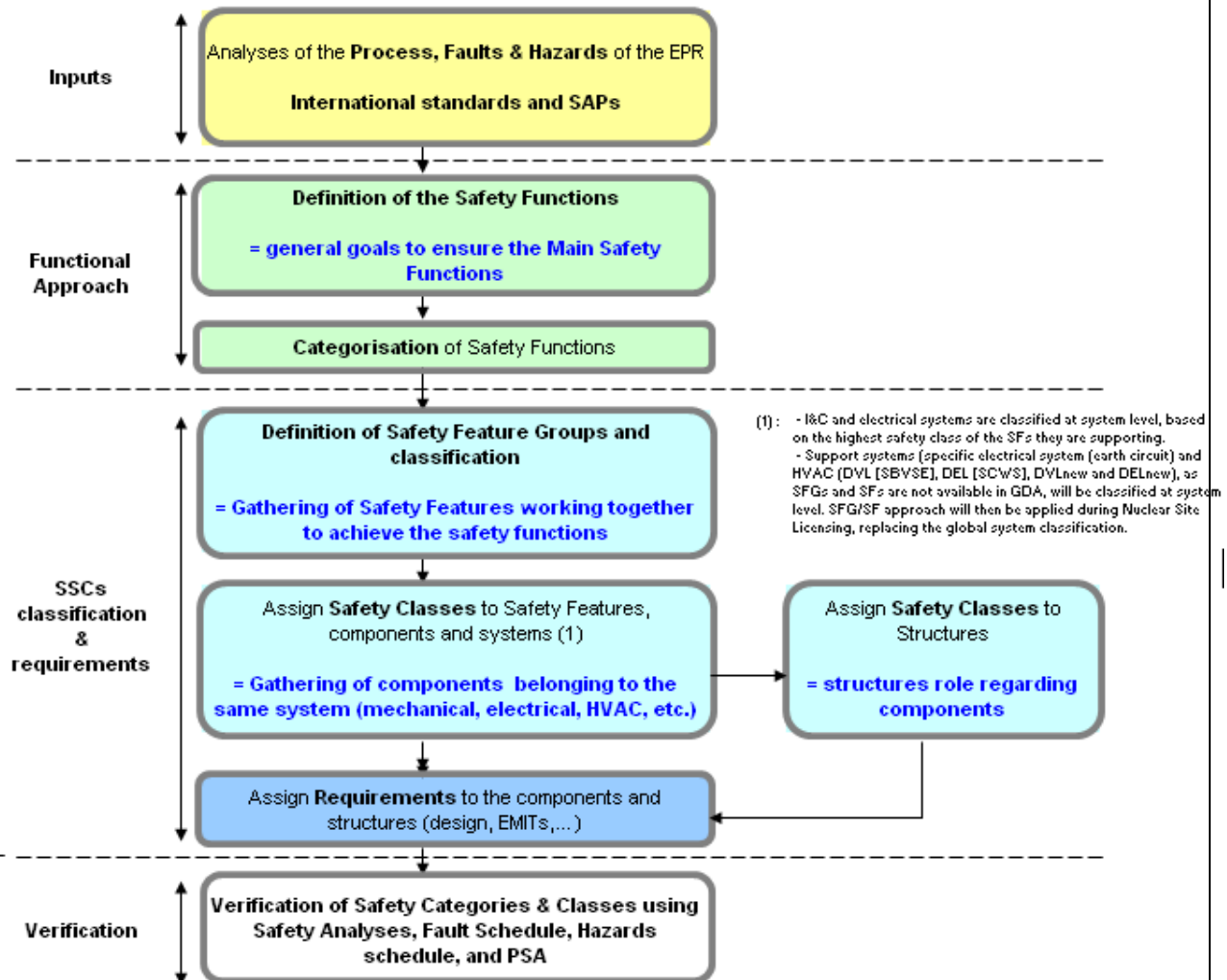
The classification methodology can be divided into four general areas:

1. Identify inputs to the classification process;
2. Categorise safety functions;
3. Classify safety feature groups, systems, safety features and components;
4. Assign requirements to safety feature groups, systems, safety features and components.

The iterative classification process is applied firstly at the concept design stage, and then reviewed during the subsequent design stages.

This methodology is practically applied as an iterative top-down process providing links from safety functions down to components. As part of this balanced classification scheme, the completeness of this top-down methodology is confirmed by applying a bottom-up check ensuring that all components of a system and all structures have been, at least once in the process, linked to a function, safety or non-safety related, that will justify its classification or non-classification. At the end of the process, depending upon the level of detail in the PSA, a PSA check will be performed to complete the analysis such that a balanced approach between deterministic and probabilistic methods is achieved.

The classification methodology is summarised below:



**2.4. ALARP PRINCIPLES AND CLASSIFICATION**

As described in detail in Chapter 17, "UK Health and Safety Legislation places a duty on all companies to conduct their operations such that the risk posed to their workers and members of the public is As Low As Reasonably Practicable (ALARP)." Chapter 17 provides information to show that the UK EPR design meets the UK ALARP requirement.

The design and manufacturing requirements resulting from the classification level assigned in the methodology are applied iteratively at each design stage, to ensure that the plant achieves the appropriate level of reliability and integrity in operation (see section 7).

Any shortfalls with respect to these classification requirements, should be justified on a case-by-case basis with an analysis performed to resolve any safety concerns, to demonstrate that no further reasonably practicable improvements could be implemented to improve the design and that the risk has therefore been reduced to ALARP.

Sub-chapter 17.5 provides operational guidance to comply with the requirements of the UK EPR ALARP methodology [Ref-2], which is based on the TAG on demonstration of ALARP [Ref-1]. In summary, an ALARP assessment corresponds to a decision making process to identify the ALARP design.

### 3. SAFETY FUNCTION DEFINITION AND CATEGORISATION

#### 3.1. DERIVATION OF SAFETY FUNCTIONS

IEC 61226 [Ref-1] defines a function as a “*specific purpose or objective to be accomplished that can be specified or described without reference to the physical means of achieving it*”. A safety function should therefore be categorised based on its safety significance.

There are three main safety functions which are necessary for achieving the overall safety objective of protecting people and the environment from harmful effects of ionising radiation:

- Control of fuel reactivity;
- Fuel heat removal;
- Confinement of radioactive material.

These main safety functions are at too high a level to allow physical solutions to be developed, so it is necessary to derive more detailed safety functions which are specific to the plant type or technology. For the EPR this has led to the development of Plant Level Safety Functions (PLSF).

#### 3.2. DEFINITION OF PLANT LEVEL SAFETY FUNCTIONS (PLSF)

PLSFs are functional capabilities based on the EPR design process, which are defined in order to satisfy the main safety functions. The PLSFs have evolved from PWR standards such as IAEA NS-R-1 Safety Requirements [Ref-1], good practice (including Sizewell B) and analysis of the EPR plant design process.

The PLSFs define at a high level the specific safety requirement or objective and do not refer to a physical means of achieving the functional and performance requirements.

A list of PLSFs is provided below:

Main Safety Function	Plant Level Safety Function
Control of fuel reactivity	R1 - Control core criticality
	R2 - Reactor shutdown and maintain core sub-criticality
	R3 - Prevent uncontrolled positive reactivity insertion into the core
	R4 - Maintain subcriticality of fuel stored outside the reactor coolant system but within the site
Fuel heat removal	H1 - Maintain Reactor Coolant System water inventory for core cooling
	H2 - Remove heat from the core to the reactor coolant
	H3 - Remove heat from the reactor coolant to the ultimate heat sink

Main Safety Function	Plant Level Safety Function
	H4 - Remove heat from fuel stored outside the reactor coolant system but within the site
Radioactive material confinement	C1 - Ensure confinement of radioactive material by fuel cladding
	C2 - Ensure confinement of radioactive material by Reactor Coolant Pressure Boundary
	C3 - Ensure confinement of radioactive material by reactor containment
	C4 - Ensure confinement of radioactive material outside of RCPB
	C5 - Ensure confinement of radioactive material from fuel stored outside the reactor coolant system
	C6 – Limit the release of (radioactive waste and airborne) radioactive material
Other	O1 - Prevent the failure or limit the consequences of failure of a component or a structure whose failure would cause the impairment of a plant level safety function
	O2 – Maintain and control environmental conditions within the plant for operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety

The pseudo main safety function (called “Other” in the table above) is defined in order to address transverse safety functions. These functions in particular relate to:

- Hazard prevention and mitigation, with functions whose failure could lead to the impairment of one or more of the original three fundamental safety functions,
- Monitoring of plant operation and conditions or other functions,
- Radiation protection functions,
- Auxiliary support to safety functions.

In order to provide a list of safety functions at an appropriate level of detail, the Plant Level Safety Functions are broken down into Lower Level Safety Functions (LLSF).

### 3.3. DEFINITION OF LOWER LEVEL SAFETY FUNCTIONS (LLSF)

The LLSF combines the objective of the PLSF with a level of defence in depth to convey the physical means of achieving the functional and performance requirements. According to the levels of defence in depth defined in the Safety principles applied to the UK EPR I&C architecture [Ref-1], the different types of NPP LLSFs identified are as follows:

- The **operational functions** (level 1 of defence in depth) which ensure **normal plant operating** conditions are maintained, with the plant parameters within their normal operating range (i.e. PCC-1 conditions, with no PCC-2, PCC-3, PCC-4 or RRC events initiated), for primary temperature control, primary pressure control, core cooling for outage, fuel handling, etc. This includes:
  - Non-safety related functions which perform a role only in industrial, non-nuclear safety related processes. These functions are screened-out of the categorisation process as they have no nuclear safety role, and their failures have no impact, on the plant safety.

- Safety related functions which perform a nuclear safety related role, even limited, as their availability is of significance to provide the first level of defence in depth (e.g. control of operating parameters within prescribed limits). The safety related functions are also commonly referred to as “duty” functions in the UK.
- The **preventive safety functions** (level 2 of defence in depth) are implemented explicitly for the **prevention**/avoidance of deviations from normal operation, following failure of functions required in normal operation (e.g. limitation function implemented to maintain important plant physical parameters within prescribed limits, prevention of hazards).
- The main line of defence in depth (level 3 of defence in depth) comprising:
  - **First line of protection** safety functions and,
  - **Diverse line of protection** safety functions for frequent postulated initiating events.

These safety functions are implemented to control the fault within the design basis by stopping the accident progression and bringing the plant to a non-hazardous stable state.

- **The risk reduction line** of defence in depth (level 4 of defence in depth) safety functions implemented to control conditions beyond the design basis including the prevention of fault progression and mitigation of the consequences of severe accident.

The Lower Level Safety Functions are categorised based on their importance to safety. The definitions for the categorisation and their assignment criteria are presented in section 3.4.

When defining the Lower Level Safety Functions, the level of detail and description should be fit for their final purpose, i.e. the classification of components.

### 3.4. LOWER LEVEL SAFETY FUNCTION CATEGORISATION

The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, are categorised based on their significance to safety. The importance to safety of a function depends on the:

- consequences of failure to perform its function;
- probability that the item will be required to perform a safety function;
- time after a postulated initiating event at which, or the period throughout which, the safety function is required.

This section provides definitions of the categories that may be assigned to safety functions. The criteria that shall be applied to the assignment of functions to categories are also provided.

Function categories are applied at the level of the Lower Level Safety Function. In other words, categories reflect the importance to safety of the Plant Level Safety Function within a specific operating condition.

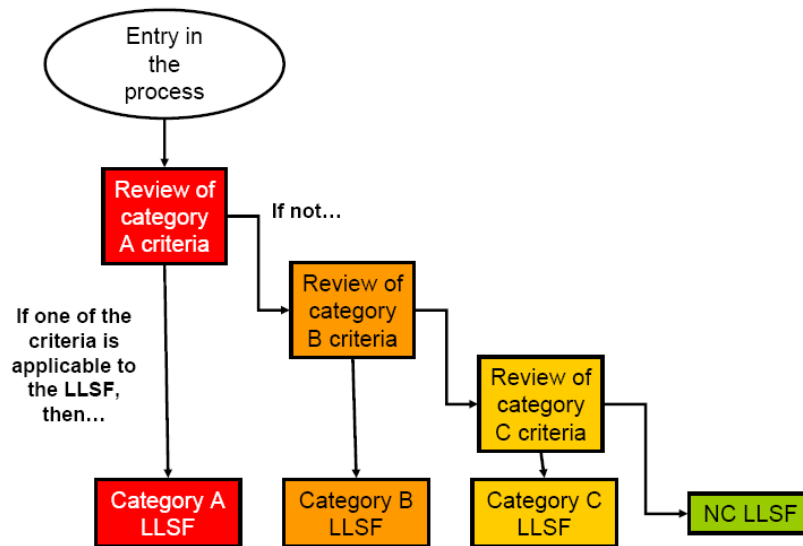


There are three categories to be considered: A, B and C. These categories are based on the definitions presented in the SAP ECS.1 [Ref-2]:

- Category A – any function that plays a principal role in ensuring nuclear safety.
- Category B – any function that makes a significant contribution to nuclear safety.
- Category C – any other safety function.

From these main definitions, the function categories are defined in detail below according to IEC 61226 [Ref-1].

The categorisation process is a top-down process, starting with the review of category A criteria and assessment of the adequacy of the criteria with respect to the importance to safety of the LLSF. The figure below illustrates this process:



**3.4.1. Category A**

According to IEC 61226 [Ref-1], “Category A denotes the functions that play a principal role in the achievement or maintenance of NPP safety to prevent DBE from leading to unacceptable consequences. This role is essential at the beginning of the transient when no alternative actions can be taken, even if hidden faults can be detected. These functions play a principal role in the achievement or maintenance of the non-hazardous stable state.

*Category A also denotes functions whose failure could directly lead to accident conditions which may cause unacceptable consequences if not mitigated by other category A functions.”*

In general, safety functions, whose failure would lead rapidly to beyond design basis consequences, and safety functions which perform an essential role in the mitigation of a design basis event are assigned to category A.

According to IEC 61226 [Ref-1], the following functions are category A:

- a) *Functions required to reach the non-hazardous stable state, to prevent a DBE from leading to unacceptable consequences, or to mitigate its consequences;*
- b) *Functions, the failure or spurious actuation of which would lead to unacceptable consequences, and for which no other category A function exists that prevents the unacceptable consequences;*
- c) *Functions required to provide information and control capabilities that allow specified manual actions necessary to reach the non-hazardous stable state [after DBE].*

#### Examples

The plant level safety function "R2 - Reactor shutdown and maintain core sub-criticality" under accident conditions leads to the definition of the lower level safety function "Negative reactivity fast insertion under PCC-2 to PCC-4 conditions". This LLSF ensures sub-criticality of the core, meeting one of the criteria of the controlled state, and is assigned to category A since it is required to reach the controlled state.

The plant level safety function "C2 - Ensure confinement of radioactive material by Reactor Coolant Pressure Boundary" under normal conditions leads to the definition of the category A lower level safety function "Prevention of RCS pressure vessel rupture".

#### **3.4.2. Category B**

According to IEC 61226 [Ref-1], "Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the non-hazardous stable state has been achieved, to prevent design basis event (DBE) from leading to unacceptable consequences, or mitigate the consequences of DBE. The operation of a category B function may avoid the need to initiate a category A function. Category B functions may improve or complement the execution of a category A function in mitigating the consequences of a DBE, so that plant or equipment damage or activity release may be avoided or minimised.

*Category B also denotes functions whose failure could initiate a DBE or worsen the severity of a DBE. Because of the presence of a category A function to provide the ultimate prevention of or mitigation of the consequences of a DBE, the safety requirements for the category B function need not be as high as those for the category A function."*

In general, the safety functions whose failure would cause a PCC-3 or PCC-4 event are usually assigned to category B unless it can be demonstrated that the subsequent PCC-3 or PCC-4 event only leads to a minor challenge to plant safety. The failure of safety functions leading to PCC-2 events cannot lead to such level of importance to safety.

According to IEC 61226 [Ref-1], the following functions are category B:

- a) *Functions required after the non-hazardous stable state of a DBE has been reached, to prevent it from leading to unacceptable consequences, or to mitigate the consequences;*
- b) *Functions required to provide information or control capabilities that allow specified manual actions necessary after the non-hazardous stable state has been reached to prevent a DBE from leading to unacceptable consequences, or mitigate the consequences;*

- c) *Functions, the failure of which during normal operation, would require the operation of a category A function to prevent an accident whose study is required;*
- d) *Functions to reduce considerably the frequency of a DBE as claimed in the safety analysis; [Although the classification of SSC, or SFG or safety related system must be fully consistent with the probabilistic and frequency claims given in section 9].*
- e) *Plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis, if these control functions are the only means of control of these variables. If different means are provided, clause a) of section 3.4.3 may apply ;*
- f) *Functions used to prevent or mitigate a radioactive release or fuel degradation outside of the limits and conditions of normal operation as defined in the safety analysis;*
- g) *Functions that provide continuous or intermittent tests or monitoring of functions in category A to indicate their continued availability for operation and alert control room staff to their failures, if no alternative means (e.g. periodic tests) are provided to verify their availability.*

#### Examples

The plant level safety function “H3-remove heat from the reactor coolant to the ultimate heat sink” under accident conditions leads to the definition of the lower level safety function “feeding water to the steam generators under PCC-2 to PCC-4 conditions”. This LLSF ensures the core cooling in the long term after reaching the controlled state, meeting one of the criteria of the safe shutdown state; it is assigned to category B.

#### **3.4.3. Category C**

According to IEC 61226 [Ref-1], “*Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes functions that have some safety significance, but are not category A or B. They can be part of the total response to DBA but not be directly involved in mitigating the physical consequences of the accident, or be functions necessary for beyond design basis accidents.*”

In general, the failures of safety functions which lead to an anticipated operational occurrence (PCC-2 event) are usually assigned to category C.

According to IEC 61226 [Ref-1], the following functions are assigned to category C (criteria C-m is applied in addition to those presented in IEC 61226):

- a) *Plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis not covered by clause e) of section 3.4.2. In case a combination of category C functions is used, a justification of sufficiency shall be provided;*

According to national practices, a possible acceptable application of clause a) of section 3.4.3 is the combination of a control function and a suitably justified manual actuation based on independent alarm(s)

- b) *Functions used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis;*

A minor release or minor fuel degradation is considered to be that which falls within the normal limits and conditions of operation (e.g. discharge limits).

- c) *Functions that provide continuous or intermittent tests or monitoring of functions in category A and B to indicate their continued availability for operation and alert control room staff to their failures, and are not classified category B according to clause g of section 3.4.2;*
- d) *Functions necessary to reach the safety probabilistic goals including those to reduce the expected frequency of a DBE; [Although the classification of SSC, or SFG or safety related system must be fully consistent with the probabilistic and frequency claims given in section 9].*
- e) *Functions to reduce the demands on a category A function, as claimed in the safety analysis;*
- f) *Functions to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);*
- g) *Functions to warn personnel or to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;*
- h) *Functions to monitor and take mitigating action following natural events [more generally external hazards] (e.g. seismic disturbance, extreme wind);*
- i) *Functions provided for the benefit of the accident management strategy to reach and maintain a safe state [final state] for beyond design accidents;*
- j) *Functions provided to minimise the consequences of severe accidents;*
- k) *Functions which provide access control for the NPP.*

It should be noticed that the licensee will implement access control arrangements in accordance with ONR (CNS) requirements.

- m) *Some additional functions which are not necessary to demonstrate the ability of the design to maintain the safe shutdown state, but which can nonetheless be required to maintain it between 24 hours and 72 hours after the event. (This criterion comes in addition to those presented in IEC 61226 [Ref-1]).*

#### **3.4.4. Non-Categorised**

Any function which does not meet any criteria of the three basic categories above is directly screened out of the categorisation process and non-categorised (i.e. functions which are considered as non-safety related).

It is important to note that boundaries and interfaces of such non safety related functions with safety functions have to be handled, at the level of systems, safety features and safety feature groups, according to the rules defined in section 4.2.

### 3.5. SAFETY FUNCTION CATEGORIES AND LLSF TYPES

The above criteria used to categorise any function are subject to interpretation, hence the following table clarifies the criteria by providing a link to the types of LLSF defined in section 3.3, thereby identifying the safety functions of the NPP and the relevant criteria to be analysed.

	Criteria	Type of LLSF		
		Operational functions	Preventive functions	Main line or risk reduction line functions
A-a	Functions required to reach the non-hazardous stable state, to prevent a DBE from leading to unacceptable consequences, or to mitigate its consequences;			YES
A-b	Functions, the failure or spurious actuation of which would lead to unacceptable consequences, and for which no other category A function exists that prevents the unacceptable consequences;	YES	YES	
A-c	Functions required to provide information and control capabilities that allow specified manual actions necessary to reach the non-hazardous stable state.			YES
B-a	Functions required after the non-hazardous stable state of a DBE has been reached, to prevent it from leading to unacceptable consequences, or to mitigate the consequences;			YES
B-b	Functions required to provide information or control capabilities that allow specified manual actions necessary after the non-hazardous stable state has been reached to prevent a DBE from leading to unacceptable consequences, or mitigate the consequences;			YES
B-c	Functions, the failure of which during normal operation, would require the operation of a category A function to prevent an accident whose study is required;	YES	YES	
B-d	Functions to reduce considerably the frequency of a DBE as claimed in the safety analysis;		YES	
B-e	Plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis, if these control functions are the only means of control of these variables.	YES		
B-f	Functions used to prevent or mitigate a radioactive release or fuel degradation outside of the limits and conditions of normal operation as defined in the safety analysis;	YES	YES	YES
B-g	Functions that provide continuous or intermittent tests or monitoring of functions in category A to indicate their continued availability for operation and alert control room staff to their failures, if no alternative means (e.g. periodic tests) are provided to verify their availability		YES	

	Criteria	Type of LLSF		
		Operational functions	Preventive functions	Main line or risk reduction line functions
C-a	Plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis not covered by B-e). In case a combination of category C functions is used, a justification of sufficiency shall be provided;	YES		
C-b	Functions used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis;	YES	YES	YES
C-c	Functions that provide continuous or intermittent tests or monitoring of functions in category A and B to indicate their continued availability for operation and alert control room staff to their failures, and are not classified category B according to B-g);		YES	
C-d	Functions necessary to reach the safety probabilistic goals including those to reduce the expected frequency of a DBE;	YES	YES	YES
C-e	Functions to reduce the demands on a category A function, as claimed in the safety analysis;		YES	
C-f	Functions to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);	YES	YES	YES
C-g	Functions to warn personnel or to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;			YES
C-h	Functions to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind);			YES
C-i	Functions provided for the benefit of the accident management strategy to reach and maintain a safe state for beyond design accidents;			YES
C-j	Functions provided to minimise the consequences of severe accidents;			YES
C-k	Functions which provide access control for the NPP.	See section 3.4.3		
C-m	Some additional functions which are not necessary to demonstrate the ability of the design to maintain the safe shutdown state, but which can nonetheless be required to maintain it between 24 hours and 72 hours after the event.			YES

## 4. CLASSIFICATION

### 4.1. IDENTIFICATION AND CLASSIFICATION OF SAFETY FEATURE GROUPS, SYSTEMS, SAFETY FEATURES AND COMPONENTS

As introduced in section 2.3, the third step of the classification approach is to identify and classify the systems, safety feature groups, safety features and components that are required to achieve the safety functions. Depending upon the situation, the physical means of achieving the functional and performance requirements could be either through a system or a part of a system that is called a safety feature. The need for a safety feature is dependent on the level of complexity of the system, with the objective to assist in the classification of individual components by grouping them according to their common role.

Typically for an I&C system as an outcome of the classification process, a safety class will be assigned at the system level, while for a mechanical system the components, within the system, that form part of the function are identified. In this way, the classification is performed at an appropriate level.

Specific terminology is defined as part of the classification process.

#### 4.1.1. System

“System” is defined in section 2.1 as the EPR coding system (ECS) as defined in the UK EPR design and corresponds to typical international usage for PWRs (e.g. main coolant system, emergency core cooling, etc.). For the UK EPR, these systems are assigned a unique ID under the ECS.

#### 4.1.2. Safety Feature

A safety feature (SF) is a part of a system that contributes to a given safety function (a LLSF as described in section 3.3). It is important to recognise that a system is typically not involved in the achievement of a single unique safety function; rather a system may have multiple safety features and provide multiple functions.

Accordingly, a safety feature is a group of components (see definition in section 2.1), actuated manually, automatically or passively, usually belonging to the same system, which contributes to the achievement of a safety function. For example, the safety feature “LHSI injection to the RCP [RCS] cold leg”, which is part of the SIS [RIS] system, is limited to LHSI pump, pipework and valves and not the entire SIS [RIS] system.

#### 4.1.3. Safety Feature Group

A safety feature group (SFG) is a concept that groups all the associated safety features that are required to ensure a safety function. Indeed, the main safety feature, also called the frontline safety feature, is grouped with a number of other safety features belonging to supporting systems (e.g. mechanical, I&C, electrical, HVAC, etc.). A safety feature group is this group of safety features, generally one frontline safety feature and its supporting safety features, which together perform a LLSF (Lower Level Safety Function).



It should be noted that:

1. The identification of the safety features of a safety feature group is an iterative process. At the end of this process, the boundaries of each safety feature and consequently those of each SFG are clearly identifiable.
2. A SFG is composed of the safety features required to ensure the LLSF; a safety feature is composed of the components required to ensure the LLSF.
3. As structures have specific functions different from mechanical, electrical and I&C components, their safety classes and associated requirements are defined in section 8.

#### 4.1.4. I&C and Electrical Systems

For I&C and electrical systems, the approach is able to provide the level of classification of I&C and electrical components that contribute to the correct functioning of the I&C and electrical systems that are identified within SFs/SFGs.

Typically, an I&C or electrical system gathers a set of identical I&C or electrical components with a common level of classification. Therefore assigning a safety class at the system level for I&C and electrical systems is more appropriate as an outcome of the classification approach.

Consistent with the SFG approach, i.e. based on the highest safety class of the SFs they are supporting, I&C and electrical systems will be assigned a safety class at the system level rather than component level.

#### 4.1.5. Other Support Systems

The classification approach developed in this document is to be applied in detail in the frame of the site licensing studies.

While SFGs and SFs are not available to provide more detailed information in GDA, support systems such as specific electrical system (earth circuit notably) and main HVAC systems (DVL [SBVSE], DEL [SCWS], DVL<sub>new</sub> and DEL<sub>new</sub>) will be assigned a safety class at the system level, based on the highest safety class of the SFs they are supporting.

SFG/SF approach will then be applied during Nuclear Site Licensing, replacing the global system classification.

## 4.2. BOUNDARIES AND INTERFACES

While defining systems, safety features and safety feature groups, boundaries and interfaces will be identified and established.

When interfaces exist between a higher and a lower safety class SFs (or SFGs), the component(s)<sup>3</sup> at the interface is (are) classified at the highest safety class in order to ensure that a failure in the SF/SFG with the lower safety class will not propagate to a higher safety classified SF/SFG.

For that purpose, specific rules are defined in section 7.4.3.2 for mechanical isolation devices of pressurised circuits, section 7.4.5 for electrical components and section 7.4.6 for I&C components.

### 4.3. SAFETY CLASSES APPLIED TO SAFETY FEATURE GROUPS, SAFETY FEATURES AND COMPONENTS

#### 4.3.1. Introduction

Safety classes reflect the importance to safety of the components contributing to a safety function performed through the safety feature groups and safety features. Consequently, the assigned safety class facilitates the design choices and represents the level of robustness that will be required in the construction and operation phases of any component. In this section, robustness is described from a design perspective (component development process, choice of technology, quality assurance level, codes and standards applied, etc.).

As recommended in DS367 [Ref-1], the classification system is independent of the technology employed. It is primarily based on deterministic methods, complemented, where appropriate, by probabilistic insights and engineering judgement with due account taken of the:

- a) category of safety function to be performed by the safety feature group;
- b) consequences of failure to perform its function;
- c) probability that the safety feature group will be required to perform a safety function;
- d) the time after any initiating fault at which, or the period during which, it will be required to operate.

#### 4.3.2. Safety Classes applied to Safety Feature Groups

In general, the safety class of a SFG should correspond to the safety category (i.e. category A corresponds to safety Class 1, category B to Safety Class 2 and category C to Safety Class 3) of the safety function (LLSF) ensured.

The safety class assigned to a safety feature group reflects the categorisation of the most important to safety LLSF (i.e. leads to the highest category LLSF) to which it contributes.

<sup>3</sup> One or several components means:

- one or two isolation components if needed,
- For mechanical safety features, one or two isolation valves and if the operation of the valve(s) is required to fulfil the isolation function, the associated electrical and I&C support components.

The mapping of the Safety Classes is the following:

- Safety Class 1 – any SFG that forms a principal means of fulfilling a category A safety function
- Safety Class 2 – any SFG that:
  - makes a significant contribution to fulfilling a category A safety function, or
  - provides a diverse means of fulfilling a category A safety function (in addition to the principal means, safety class 1 SFG that fulfils the function) or
  - provides a principal means of ensuring a category B safety function.
- Safety Class 3 – any SFG that:
  - contributes to a category B function in addition to a safety class 2 SFG, or
  - provides a principal means of ensuring a category C function.

#### 4.3.3. Safety Classes applied to Safety Features and Components

As a general principle, a safety feature will be classified at the same level as the most highly classified SFG to which it contributes. Accordingly, the components belonging to a safety feature will be classified at the same level as the safety feature.

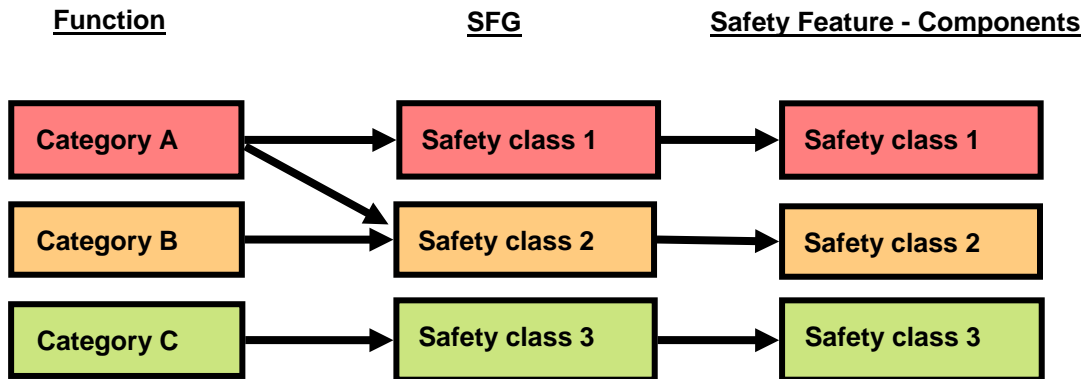
When redundancy is required between two components, both are classified identically.

In certain circumstances, there may be a limited number of safety features (or components) that are one class lower than the SFG (or safety feature) to which they contribute. In such cases, adequate justification must be provided to demonstrate that this lower class is the suitable one through an ALARP analysis. Judgement must be exercised taking into account such factors as, but not limited to:

- the importance of the safety feature (or component) (e.g. whether it is required to reach the non-hazardous stable state or required after);
- whether or not a malfunction would affect the safety function it delivers; and
- whether or not a malfunction of the equipment would be revealed during normal operation.

**4.3.4. Overview of Safety Classes applied to Safety Feature Groups, Safety Features and Components**

The figure below presents an overview of the classification process.



It should be noted that:

1. The arrows show the main links between functions, SFGs, safety features and components, whereas in certain circumstances (see above) and only where adequate and acceptable justification can be provided, it is appropriate for a safety feature (component) that is one class lower than the corresponding category of safety function to contribute to that safety function.
2. The arrows from category A to safety class 1 and safety class 2 indicates that a category A function may be fulfilled by a safety class 1 SFG fulfilling the first line of protection and a safety class 2 SFG that acts as a diverse line of protection. A diverse line is required for frequent faults.

**4.4. SAFETY CLASSES APPLIED TO SYSTEMS**

Under the explanations and conditions developed in sections 4.1.4 and 4.1.5, I&C systems, electrical systems and other support systems will be assigned a safety class at the system level, based on the highest safety class of the SFs/SFGs they are supporting (see section 4.3.3) as an outcome of the classification approach.

**5. ARCHITECTURE REQUIREMENTS APPLIED TO SAFETY FEATURE GROUPS**

As introduced in section 2.3, the fourth step of the classification approach is to link the classification to a set of requirements.

Architecture requirements applied to SFGs are essential for designing robust lines of defence consistent with their importance to safety, captured in the safety class. Such requirements strengthen the system design:

- against single faults and associated consequences (Single Failure Criterion) by requiring redundancy, physical separation;
- by ensuring its availability in the requested situation (qualification, protection against hazards including seismic requirements);
- by providing high availability of the SFG either intrinsically through high reliability or through the application of periodic tests in plant operation.

The level of architecture requirements is derived from the category of functions (A, B or C) to be achieved and is assigned to safety feature group.

As stated previously in section 3.3, there are different types of functions according to each level of defence in depth, consequently, the level of architecture requirements are defined per line of defence for a given SFG, as described in sections 5.2.1 to 5.2.4. Before detailing these requirements, a brief introduction to the set of architecture requirements is provided in section 5.1.

The level of architecture requirements depicted in sections 5.2.1 to 5.2.4 shall be achieved in order to ensure an adequate and reliable design. If, in a few cases these requirements could not be met, the adequacy of the proposed design shall be demonstrated through an ALARP analysis (see section 2.4).

Some requirements are assigned at the SFG level (e.g. robustness against single failure, physical separation and EMIT); whereas, robustness against earthquake, robustness against LOOP and qualification for accident conditions are also assigned at the component level.

As structures have specific functions different from mechanical, electrical and I&C components, the requirements applicable to structures are defined in a dedicated section 8.

## 5.1. DEFINITION OF THE ARCHITECTURE REQUIREMENTS

### 5.1.1. Robustness against Single Failure - Redundancy

The UK EPR definition of single failure is given in section 2.1 and is based on the redundancy requirement defined in Sub-chapter 3.1:

*"[...] This requirement for redundancy assists in ensuring high reliability of safety classified safety feature groups designed to maintain the plant within its deterministic design basis.[...] The single failure taken into account is a random failure independent of the initiating event [...] A short term single failure of a component belonging to the safety feature group is considered for both active components and passive components."*

The passive and active failures to be considered are defined in detail in Sub-chapter 3.1.

Generally, the passive single failure is considered through the active components of the SFG. As an example the passive failure of a pipe on a closed pipe and pump single circuit has similar effects as the failure of the pump, i.e. the circuit is not providing water.

In the particular case, if the failure of a passive component is not assumed and is not encompassed by an active failure, adequate and acceptable justification must be provided through an ALARP analysis to demonstrate that this is acceptable. Judgement must be exercised taking into account, but not limited to, such factors as those described in IAEA NS-R-1 [Ref-1]: *“In the single failure analysis, it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality, provided that it remains unaffected by the PIE. However, when it is assumed that a passive component does not fail, such an analytical approach shall be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary”*.

### 5.1.2. Physical Separation

As defined in section 2.1, physical separation relates to a *“Separation by geometry (distance, orientation, etc...) or by appropriate Barriers or by a combination thereof”*. The need for physical separation comes from the need to prevent common cause failures of redundant parts of a system resulting from a hazard (fire, explosion or flooding for example). It strengthens confidence in the ability to deliver a safety function notably in the event of a hazard affecting an SFG.

Physical separation should preferably rely on the use of separate structures. In the event that such separation is not achievable (e.g. emergency and ultimate diesel generators may supply power to the same component), sufficient provisions (separation distances) should be provided to limit as much as possible potential common cause failures due to hazard.

### 5.1.3. Robustness against LOOP

The main and the auxiliary grid supply electrical power under normal plant conditions. However, during a natural event (earthquake, extreme weather conditions) or a grid fault, a loss of offsite power event (LOOP) may occur.

The occurrence of LOOP must not result in the loss of capability of an SFG to perform its intended post LOOP safety functions.

Robustness against LOOP of a given SFG can be ensured by using a failsafe design or by connection of single components to the Emergency Power Supply.

### 5.1.4. Robustness against Earthquake

To preclude significant impact on plant safety, the designer must take into account the seismic characteristics of the site where the NPP is being built and provide the SFG with relevant seismic requirements. Sub-chapter 13.1 describes the seismic design principles of the UK EPR.

Similarly to LOOP, occurrence of an earthquake must not result in the loss of capability of an SFG to perform its intended post-earthquake safety functions.

Robustness against earthquake of a given SFG must be demonstrated by using a failsafe design or by ensuring adequate design and manufacturing requirements of single components (SC1/SC2 as defined in section 7.1) to achieve proper operation in the event of a seismic event.

### 5.1.5. Qualification for Accident Conditions

The objective of qualification for accident conditions is to demonstrate that an SFG would be able to fulfil its safety functions in accident conditions considering all the postulated environmental conditions and loads to which it may be subjected (normal, incident, accident conditions including hazards).

This design aspect is set out in Sub-chapter 3.6 for PCC events and in Chapter 13 for hazards.

### 5.1.6. Examination, Maintenance, In-Service Inspection, Testing (EMIT)

Periodic testing of SFGs is necessary to confirm their availability and ensure their reliability consistently with their performance requirements. Such periodic testing is mandatory for safety features important to safety which are not continuously in operation in normal plant conditions. More generally, periodic testing also encompasses Examination, Maintenance, In-Service Inspection (EMITs). Sub-chapter 18.2 of provides further insights into what EMITs are and how they are established.

## 5.2. ARCHITECTURE REQUIREMENTS PER LINE OF DEFENCE

The table at the end of this section provides the architecture requirements applicable to the SFG. Such requirements are given per level of defence to deliver the different types of LLSF as defined in section 3.3. The following sections give details and rationales, for any specific application of each architecture requirement per lines of defence.

### 5.2.1. Normal Operation or Preventive lines

**Robustness against single failure - redundancy:** Only required for safety class 1 SFG. In practice, such SFGs would mainly be composed of passive High Integrity Components (Sub-chapter 3.4), for which gross failures are excluded from the design and the single failure criterion would not apply. For safety classes lower than safety class 1, robustness against single failure is not required, but may be applied in the design of safety class 2 to ensure reliability commensurate with their importance to safety.

**Physical separation:** If robustness against SFC is required.

**Robustness against LOOP:** Only required for safety class 1. In practice, the SFG is usually composed of passive components and thus this requirement may not be relevant. As no single failure criterion is retained for lower safety classes, the robustness against LOOP is not required.

**Robustness against earthquake:** A seismic event should not lead to the failure of a classified SFG whose failure would have unacceptable consequences. Not only must such SFG be able to withstand seismic loads but they should also be designed to ensure their safety function afterwards (e.g. the RPV must not lose its integrity in a design basis earthquake – gross failure would be unacceptable). For safety class 2 and 3 robustness against earthquake is not required but an analysis at the component level is necessary to assess the actual seismic requirements.

**Qualification for accident conditions:** Not applicable to operational and preventive functions as they are not required to operate under accident conditions.

**EMIT:** Required for safety classified SFGs, to be commensurate to the safety role.

### 5.2.2. First Line of Protection

**Robustness against single failure - redundancy:** Required for safety class 1. This means that such SFG necessarily contain redundant elements. For safety class 2 the single failure criterion (active or passive) is applied at the level of the LLSF. This means that such SFG do not necessarily contain redundant elements and when they do not, another safety function must be assessed to demonstrate compliance with the single failure criterion. In this case, a requirement for physical and electrical separation is applied to the other function. For safety class 3, a functional analysis may conclude on the need to apply the SFC. Note that the analysis of internal hazards considers a single failure.

**Physical separation:** If robustness against SFC is required.

**Robustness against LOOP:** Required for safety class 1 and 2. For some safety class 3, it may be required where the SFG is needed for hazard protection (fire, earthquake, external flooding, extreme temperatures and hazards linked to the industrial environment).

**Robustness against earthquake:** Required for safety class 1 and 2.

**Qualification for accident conditions:** Required for all safety classified SFGs.

**EMIT:** Required for all safety classified SFGs.

### 5.2.3. Diverse Line of Protection

The diverse line is generally provided by safety class 2. Therefore the requirements will be defined at this level of classification.

**Robustness against single failure - redundancy:** Not required since the safety function is already being ensured by diverse means (first line and diverse line of protection).

**Physical separation:** Not required, consistent with SFC requirement.

**Robustness against LOOP:** Required only if used in LOOP accidents.

**Robustness against earthquake:** May be required on a case-by-case basis.

**Qualification for accident conditions:** Required for all safety classified SFGs.

**EMIT:** Required for all safety classified SFGs.

### 5.2.4. Risk Reduction Line

The risk reduction line is ensured by safety class 3 and safety class 2 SFGs. There are no safety class 1 SFGs designed for the unique purpose of providing a risk reduction line of protection.

**Robustness against single failure - redundancy:** Generally not required, may be required if redundancy is necessary to achieve the reliability claim of safety class 2 systems (especially for I&C components).

**Physical separation:** If robustness against the SFC is required.

**Robustness against LOOP:** Required only if used in LOOP accident.



**Robustness against earthquake:** May be required on a case-by-case basis. Generally, in this line of protection, the SFGs that take part in severe accident mitigation are designed to withstand an earthquake.

**Qualification for accident conditions:** Required for all safety classified SFGs.

**EMIT:** Required for all safety classified SFGs.

### **5.3. SUMMARY OF ARCHITECTURE REQUIREMENTS PER LINE OF DEFENCE**

See table below:

SFG safety class	Robustness against single failure redundancy	Physical separation	Robustness against LOOP	Robustness against earthquake	Qualification for accident conditions	EMITs
------------------	--	---------------------	-------------------------	-------------------------------	---------------------------------------	-------

**Normal plant operation and prevention**

See section 5.2.1	1	Yes	Yes	Yes	Case-by case at the component level	N/A	Yes
	2	No	No	No	Case-by case at the component level	N/A	Yes
	3	No	No	No		N/A	Yes

**First line of protection**

See section 5.2.2	1	Yes	Yes	Yes	Yes	Yes	Yes
	2	Yes	Yes	Yes	Yes	Yes	Yes
	3	No	No	No	Case-by-case at the level of components	Yes	Yes

**Diverse line of protection**

See section 5.2.3	2	No	No	No except if SFG used in LOOP accidents	Case-by-case at the component level	Yes	Yes
-------------------	---	----	----	---	-------------------------------------	-----	-----

**Risk reduction line**

See section 5.2.4	2	No, except to reach safety class 2 reliability claim of PSA		No except if SFG used in LOOP accidents	Case-by-case at the component level	Yes	Yes
	3	No					

## 5.4. ARCHITECTURE REQUIREMENTS BETWEEN LINES OF DEFENCE

This section provides requirements applicable to the SFGs that have to be implemented between lines of defence, in addition to those in section 5.2.

Requirements such as defence in depth, independence, and diversity that apply between lines of defence shall be provided. The main requirement that is applicable at the SFG level (i.e. I&C, electrical and, mechanical components) is a diversity requirement between SFGs implemented in the first and the diverse lines of protection. Functional diversity analysis performed in Sub-chapter 16.5 provides justification for the compliance of the UK EPR design with this requirement such that adequate architecture requirements are implemented between lines of defence.

## 6. REQUIREMENTS APPLIED TO SYSTEMS

When a safety class is applied for a support system at system level rather than safety feature level as depicted in section 4.4, the requirements to be applied to the components of the system can be either:

- Applied at component level as depicted in section 7. For example, for HVAC system involving mechanical, electrical the use of different design codes and requirements are to be defined and component level is appropriate,
- Applied at system level considering the rules depicted at component level in section 7. For example, for I&C systems, the components involve similar design codes and requirements and system level is appropriate.

## 7. REQUIREMENTS APPLIED TO COMPONENTS

Requirements are applied at the component level by covering the following design aspects:

- Derived from architecture requirements:
  1. Robustness against Earthquake (developed in section 7.1);
  2. Robustness against LOOP (developed in section 7.2);
  3. Qualification for accident conditions (developed in section 7.3);
- Specific to components:
  4. Design codes and other manufacturing requirements (developed in section 7.4)
  5. Level of quality assurance (developed in section 7.4.7);

The requirements applied to a component depend on its safety classification, which in turn depends on the safety classification of the most highly classified safety feature to which it contributes.

The levels of requirements depicted in the next sections shall be achieved in order to ensure an adequate and reliable design of each component. If, in a few cases these requirements could not be exhaustively met, an analysis shall demonstrate that the proposed design is ALARP (see section 2.4).

In particular, on a case-by-case basis, taking into account the less important role in nuclear safety of a safety class 3 safety feature, and provided that adequate and acceptable justification can be presented, through an ALARP analysis, it may not be appropriate to impose all the specific design requirements on the components of this safety feature (with the exception of quality assurance which would still need to be applied).

An example could be a category C function fulfilled by a safety class 3 SFG which includes a safety class 3 safety feature, whose components from the conventional island are subject to quality assurance requirements (section 7.4.7), but are designed to an alternative industrial design standard. This decision would be based on considerations such as:

- there are few, if any, changes needed to the normal operational configuration of the safety feature to achieve the safety function after the initiating event and its safety function would not be affected by it,
- the safety feature makes only a negligible contribution to risk reduction.

This is generally the case for functions ensured under normal operation by safety related components.

As structures have specific functions different from mechanical, electrical, and I&C components, the requirements applicable to structures are defined in a dedicated section 8.

## **7.1. ROBUSTNESS AGAINST EARTHQUAKE**

Consistent with Sub-chapter 13.1, the robustness against earthquake applicable to a component depends on:

- the safety role, of the SFG it belongs to, during and following an earthquake,
- the consequences on classified components of its failure, if it were not robust against earthquake.

Two levels of seismic requirements are defined for that purpose SC1 and SC2:

- SC1 represents the set of seismic requirements which ensure that a safety function needed to bring the plant to a non-hazardous stable state and maintain it can be delivered, in the case of earthquake,
- SC2 represents the set of seismic requirements which ensure there is no damage (failure of adjacent equipment or internal hazards induced) on adjacent SC1 components, resulting from the earthquake.

The fundamental requirements which may be applied to components are:

- operability,
- functional capability,

- integrity,
- stability.

### 7.1.1. Components subject to SC1 Requirements

Components subject to SC1 requirements are discussed below.

- SC1 requirements are usually applied to all components belonging to SFGs of the first line of protection with a requirement of robustness against earthquake (see “YES” in the table of section 5.3) except mechanical components that perform a barrier role, to which SC1 requirements are applied only on a case-by-case basis, taking into account whether the containment function is performed by the component itself or by the design of the building,
- SC1 requirements do not apply to safety classified (1, 2 and 3) components which are used only in normal operation state, to which SC2 requirements are applied, on a case-by-case basis (see below),
- SC1 requirements do not usually apply to safety class 3 SFGs and components, except for:
  - Mechanical components that perform a barrier role, to which SC1 requirements are applied only on a case-by-case basis, taking into account whether the containment function is performed by the component itself or by the design of the building,
  - Containment heat removal SFG and components used in severe accident (RRC-B conditions),
  - Partitions, fire detection and fire-fighting components installed in safety class 1 buildings which contain safety class 1 SFGs and components,
  - Systems that may be required to sustain the safe shutdown state for periods of between 24 and 72 hours.
- For other safety class 1 and 2 components, SC1 requirements apply on a case-by-case basis depending on the safety role, during and following an earthquake, of the SFG to which they belong. For example, related to SC1:
  - Ultimate Diesel Generators (UDG) sets (i.e. the diesel generator sets used in the event of loss of off-site power conditions combined with failure of the main diesel generators).
  - and their associated components.

Design of components with SC1 requirements involves at least “stability”.

**Stability** is the ability of a component to resist loads which have a tendency to modify its position or orientation (for example, which have a tendency to cause the component to tilt, fall or slide in an unacceptable manner or which could lead to a breakage of the component). The stability of a component relies upon the stability and resistance of its supports.

Electrical and I&C components, SC1 requirements usually involve "operability after an earthquake".

**Operability** is the ability of a component, consistent with the other components of the safety feature and safety feature group to which it belongs, including auxiliaries, supports and electrical power supplies, to perform the SFG safety function and meet the safety objectives.

Mechanical components, SC1 requirements usually involve "functional capability" or "operability" functions after an earthquake. For mechanical components if SC1 requirements apply exclusively due to a barrier role, only "integrity" is required.

**Functional Capability** is the ability of a component in a pressurised system to resist the specified loads with limited deformation such that its operational capacity is not impaired by a possible flow reduction. It is defined consistent with the safety function of safety feature group to which it belongs.

**Integrity** is the ability of a component in a pressurised system to resist the specified loads without leakage.

### 7.1.2. Components subject to SC2 Requirements

The following components are subject to SC2 requirements:

Safety classified components, not already SC1, which have a protection role towards SC1 components, or whose failure (if they were not robust against earthquake) in a seismic event could have an unacceptable impact on SC1 component. An 'unacceptable impact' could arise if one of the following consequential internal hazards was caused by the seismic motion:

- Equipment toppling or falling on equipment with SC1 requirements,
- Missile generation,
- Effects caused by high energy component failures,
- Flooding caused by failures of pipework, tanks or reservoirs,
- Explosion (according to ETC-F),
- Fire (according to ETC-F).

Analysis of the consequences of failure that could be caused by an earthquake must take into account the possibility of multiple failures.

Consequential failures caused by the failure of electrical and I&C equipment must be prevented by the decoupling between protected and non-protected parts.

In particular, if the earthquake could lead to an internal hazard, the provisions for dealing with this internal hazard or the measures to prevent it, must comply with SC2 requirements.

SC2 components are to be designed using methods appropriate to their intended use. SC2 requirements usually involve "stability" and or and/or "integrity", as defined above.

## **7.2. ROBUSTNESS AGAINST LOOP**

Requirements for robustness to LOOP at the level of components depend on the SFGs they belong to. No further specific requirements apply (see section 5.1.3 for details).

## **7.3. QUALIFICATION FOR ACCIDENT CONDITIONS**

Requirements for qualification against accident conditions at the level of components depend on the SFGs they belong to. No further requirements apply (see section 5.1.5 for details).

## **7.4. COMPONENT REQUIREMENTS**

### **7.4.1. Types of Components to be Classified**

The components in the UK EPR design can be grouped into a number of types for the purpose of allocating the codes and standards which they need to satisfy. The following groupings have been identified:

- Pressure retaining components:
  - Pumps,
  - Tanks,
  - Valves,
  - Pipework,
  - Heat exchangers,
- Non-Pressure retaining components:
  - Supports of pressure components and electrical components,
  - Vessel internals,
  - Mechanical components of ventilation systems,
  - Component that are parts of handling devices,
  - Fuel assembly and Reactor Cluster Control Assembly,
- Electrical and I&C equipment.

Some components, such as motorised valves or pumps, may not fall within the above groups of a given single type. In such cases, design requirements, codes and standards applied must be adequately chosen in the following sections to reflect exhaustively all the different aspects of the design (electrical part, mechanical part, etc.).

### 7.4.2. General Requirements for Components

The general requirements applicable to classified components are as follows:

- Design and construction must follow specific common codes and standards (see Sub-chapter 3.8 for the RCC-M, RCC-E, ETC-F and ETC-C codes). These common codes and standards define the methodologies, rules and criteria to be used for design, construction, procurement, installation, inspection and testing of the components.
- A quality assurance programme is to be followed. QA programmes must be applied at the different stages of component life (design, construction, procurement, installation, inspection, testing, operation, modification).

### 7.4.3. Mechanical Requirements for Pressure Retaining Components

The mechanical requirements applicable to pressure retaining components depend on the following:

- Safety classification of the component; and
- Confinement of radioactivity: potential for the release of radioactivity as a result of the failure of the component (i.e. failure of its barrier role). Components, whose failure can, under normal and accidental conditions (operational conditions PCC-1 to PCC-4 and RRC-A or RRC-B) lead to a discharge of radioactivity significantly greater than that existing in the surrounding environment, are subject to mechanical requirements (M1/M2/M3).

To ensure the functional capability of mechanical components, appropriate codes or standards are applied in the design and manufacturing of the equipment so that the component quality is appropriate to the function that it provides.

The mechanical requirements include provisions for the application of a Quality Assurance programme, qualification required for specific operating conditions, seismic qualification, and periodic testing/in-service inspection.

#### 7.4.3.1. Assignment of Component Mechanical Quality Requirements (M)

Three mechanical requirement levels (M1, M2 and M3) are defined for pressure retaining components with the demonstration of an appropriate level of mechanical requirements achieved through application of a combination of safety class and barrier role as follows:

Firstly, the safety class drives the minimum requirements to be applied:

- Safety class 1 and Safety class 2 components must meet M3 requirements at least,
- Safety class 3 components do not need to meet M1, M2 or M3 requirements (i.e. 'M' requirements not needed).



Secondly, the operating conditions and barrier role give the following requirements:

- M1 requirements:
  - The component forms the Reactor Coolant Pressure Boundary (RCPB)<sup>4</sup>,
  - The component is a High Integrity Component (HICs are listed in Sub-chapter 3.1 and Sub-chapter 3.4 section 0).
- M2 requirements:
  - The component performs a barrier role. The component is required to maintain its pressure boundary integrity during conditions where the component is not isolated from the primary coolant circuit under PCC or RRC conditions where cladding damage may have occurred ( see definition below),
  - The component forms part of a Reactor Building penetration, unless already identified as HIC (M1).
- M3 requirements:
  - The component performs a barrier role: its failure could potentially, under normal or accident conditions (PCC-1 to PCC-4 and RRC conditions), lead to a discharge of radioactivity significantly greater than that existing in the surrounding environment<sup>7</sup>.

The following definitions apply in the interpretation of the above criteria:

- "Required" refers to the component belonging to or being part of a system required to perform the safety function under PCC or RRC conditions.
- "Cladding damage may have occurred" refers to acceptance criteria applicable to the Plant Condition or Risk Reduction Category being considered (Chapter 14 for PCCs and Sub-chapter 16.1 for RRC-A). Despite demonstration that clad damage does not occur in the results of the specific accident studies, the applicable criteria (acceptance criteria from the considered PCC/RRC events) are adopted as conservatism.

<sup>4</sup> M1 is not applicable to pipework whose failure (e.g. pipe break) can be compensated for by the make-up capacity of the RCV [CVCS].

<sup>7</sup> Activity is considered as being significantly greater than that existing in the surrounding environment when the following two conditions occur:

- The activity concentration of the fluid concerned exceeds 1 MBq/l
- The activity concentration of the fluid concerned exceeds that existing in the environment by a factor of 1000.

These thresholds are proposed on the basis of values observed in natural radioactivity (approximately 1 to 10<sup>3</sup> Bq/kg). Such thresholds exclude components which contain low-activity fluids, as well as systems that operate only inside the containment in conditions where the containment environment is degraded.

**7.4.3.2. Specific Components: Isolation devices**

As defined in section 4.1.3 when interfaces exist between a higher and a lower safety class safety feature (or SFG), the mechanical component(s) at the interface is (are) classified at the highest safety class. Their requirements shall be defined accordingly and adequately in order to ensure that a failure from the lower safety class

- does not prevent the highest safety function from being performed,
- does not result in the uncontrolled release of radioactive gases normally stored for decay.

When an isolation component, whether motorised or not, is used to separate two sections of a mechanical system with different mechanical requirements (e.g. M1 and M2 pipework separated by an isolation component or M2 and NR<sup>8</sup>...), the following additional requirements apply:

- If the isolation component is redundant, the same requirements apply to both the isolation valves and to the part (e.g. pipework) of the mechanical system which may link them.
- The isolation component(s) inherits the highest safety requirements of the two sections of the system which it separates.

The possible interfaces between mechanical pressure retaining components are defined in the table below, which is based on the French NPP fleet experience and EPR basic design considerations:

Highest mechanical requirement	Possible interface	Lowest mechanical requirement
M1 (1)	At least: <ul style="list-style-type: none"> <li>- a pressure relief valve or</li> <li>- two active components (remote control motor operated valves or check valves) in series or</li> <li>- two usually closed valves, in series,</li> <li>- A flow-limiting orifice (2).</li> </ul>	M2, M3, NR
M2	At least: <ul style="list-style-type: none"> <li>- a pressure relief valve or</li> <li>- a remote control motor operated valve (3) or</li> <li>- a check valve (3) or</li> <li>- a usually closed valve or</li> <li>- an exchanger wall or</li> <li>- a fixed point (4) or</li> <li>- nothing (4)</li> </ul>	M3, NR
M3	As for M2	NR

<sup>8</sup> No mechanical Requirement

- (1) A limited number of safety classified components are HIC and upgraded to the M1 requirement. In that particular case the M level to be taken into account in this table is the level before application of M1 HIC. An example could be the steam generators: M2 for their barrier role in SGTR accident conditions, but M1 because of HIC requirements.
- (2) The use of a flow-limiting orifice shall only be acceptable for small diameter pipework, i.e. pipework where the presence of the orifice ensures that, in the event of failure the leak (limited by the flow-limiting orifice) can be compensated for by normal make-up means.
- (3) Utilisation of a single component may be appropriate provided that the failure to close this component cumulated with the failure of the lower classified system of the interface does not impair the safety function(s) of the interfacing higher classified system and does not allow an uncontrolled release of radioactive gases, stored to decay, to occur. If this is not ensured, then two isolation components will be necessary.
- (4) Provided that the failure of a lower class component will not prevent the higher safety class component from achieving its safety function, nor result in the uncontrolled release of radioactive gases normally stored for decay.

#### 7.4.3.3. Application of RCC-M Code and European Standards

The mechanical requirements M1, M2 and M3 relate directly to the level of design code or standard to be applied. The mechanical requirements for pressurised equipment imply the following design codes / standards:

- M1 requires the application of RCC-M1;
- M2 requires the application of RCC-M2 or ASME III with supplements or KTA with supplements;
- M3 requires:
  - Application of nuclear code RCC-M3 (or another nuclear code) for safety class 1 and 2 components.
  - Application of RCC-M3, or European Harmonised Standards with supplements or any code compliant with PED, with supplements, for safety class 3 components.

The application of RCC-M code (or equivalent – See Sub-chapter 3.8) ensures there are sufficient design margins to provide adequate integrity and mechanical stability for the components. A limited number of safety classified components will not be designed according to RCC-M (or equivalent), but similar high standards will be adopted. Typically in such cases, a well-established design is available and a change of design code would be counter-productive. An example could be a non-HIC component on the conventional island.

#### 7.4.3.4. Summary

The table below summarises the relationship between the safety class, the mechanical requirements and the standards applied.

Component Safety Class	Part of RCPB or HIC?	Mechanical Component requirement	Design code
1	Yes	M1	RCC-M1
	No	M2	RCC-M2 or ASME III with supplements or KTA with supplements
	No	M3	RCC-M3
2	No	M2	RCC-M2 or ASME III with supplements or KTA with supplements
	No	M3	RCC-M3
3	No	M2	RCC-M2 or ASME III with supplements or KTA with supplements
	No	M3	RCC-M3 or Harmonised European standards with supplements (or any code compliant with PED, with supplements)
	No	NR	Harmonised European standards (or any code Compliant with PED)

**7.4.4. Mechanical Requirements for Non-pressure Retaining Components**

In the case of non-pressure retaining components, the M1, M2 and M3 mechanical requirements described in section 7.4.3 are not appropriate and therefore not applied. Thus, they are replaced by other mechanical requirements, as described below.

The mechanical requirements include provisions for the application of a Quality Assurance programme, the degree of qualification for particular operating conditions, seismic qualification, and periodic testing/in-service inspection.

**7.4.4.1. Assignment to Non-pressure Retaining Component Requirements**

For mechanical components that are not pressurised, precise requirements are defined in dedicated technical specifications (i.e. BTS for most duty systems notably), which may be specific to an individual piece of equipment or may apply to a component type. Such requirements are usually tailored according to the safety class of the component as defined in section 4. In particular, for non-pressure retaining components several measures are taken into account (sound design, use of proven materials, integrity analysis, high standards of manufacture, in-service inspections, etc) to prevent any risk of failure.

**7.4.4.2. Application of Codes and Standards**

The quality of most non-pressure retaining components is ensured by application of requirements defined in the BTS as mentioned in section 7.4.4.1. However, some components require the application of specific codes as defined below.

#### **7.4.4.2.1. Supports of Fluid System Components**

The criteria applicable to supports are based on the principle that the supports of a fluid component are as important as the component being supported. Consequently, the classification process explicitly considers them, as follows.

Requirements on supports are divided into three sub-levels:

- supports of M1 components: the requirements of the dedicated RCC-M sub-section are applied (Volume H, requirements for S1 supports),
- supports of M2 components: the requirements of the dedicated RCC-M sub-section are applied (Volume H, requirements for S2 supports), or equivalent requirements from another nuclear code (ASME section III or KTA),
- supports of M3 components: the requirements of harmonised European standards are applied or equivalent industrial practices compliant with the PED (if it is decided to use RCC-M, requirements for S2 supports will be applied).

The supports of large RCC-M valve motors and large RCC-M pump motors are considered as supports for the corresponding RCC-M components.

The supports of other electrical equipment (cables, connections, electrical cabinets, etc.) are addressed within the RCC-E, with supports adequately designed based on their functional purpose/role.

The equipment internal to fuel pools utilises M2 component supports.

Design rules for supports or support components which are embedded in concrete (anchorage) are part of the structures and given within ETC-C (see Sub-chapter 3.8) for classified structures.

#### **7.4.4.2.2. Reactor Pressure Vessel Internals**

With regard to their contribution to safety, the reactor pressure vessel internals are divided into two sub-classes:

- core support structures (CS),
- other internal structures (IS)

CS components are those that are necessary to ensure the mechanical integrity of the fuel assemblies.

The vessel internals are covered by a dedicated sub-section of RCC-M (volume G), which specifies applicable design rules in accordance with the CS/IS classification.

#### **7.4.4.2.3. Fuel Assemblies and Rod Cluster Control Assemblies**

For fuel assemblies and Rod Cluster Control Assemblies (RCCA), the M1, M2, M3 mechanical quality requirements are not relevant. These components are designed according to the dedicated standard RCC-C (see Sub-chapter 4.2).

#### **7.4.5. Electrical Component Requirements**

Electrical requirements are only applied to electrical components of an SFG/safety feature that have the operability functional requirement.

The level of design requirements associated to electrical components follows its safety class:

- C1: electrical components Safety class 1;
- C2: electrical components Safety class 2,
- C3: electrical components Safety class 3.

RCC-E provides the basis for the requirements, supplemented by a dedicated Book of Technical Specifications and international standards commensurate with the importance to safety of the electrical components.

A limited number of safety classified components will not be designed to the RCC-E code, but similar appropriate high standards will be adopted and justified by an ALARP analysis. Typically in such cases, a well-established design is available and trying to apply RCC-E would be counter-productive. An example could be a safety class 3 component on the conventional island, already designed for other nuclear and non-nuclear power plants.

When interfaces exist between a higher and a lower class electrical component, the component at the interface is designed in order to ensure that a failure will not propagate from a lower safety class component to higher safety classified components.

#### **7.4.6. I&C Component Requirements**

I&C requirements are only applied to I&C components of an SFG/safety feature that have the operability functional requirement.

The design requirements applicable to I&C components depend on the safety class of the SFG they contribute to:

- C1: I&C components Safety class 1 (cat. A requirements of IEC61226:2009),
- C2: I&C components Safety class 2 (cat. B requirements of IEC61226:2009),
- C3: I&C component Safety class 3 (cat. C requirements of IEC61226:2009).

Regarding the codes and standards that apply to I&C components, the basis is RCC-E complemented by IEC standards when relevant. Production Excellence and Independent Confidence Building Measures commensurate with the safety class of the components must be provided for digital I&C as defined in the UK EPR guideline [Ref-3] and the safety principles applied to the UK EPR I&C architecture [Ref-1] for computer based components.

If the I&C component is integrated within an electrical component (e.g. smart device within a busbar), the I&C requirements and standards defined in the applicable code (RCC-E), complemented by IEC standards when relevant, apply to the I&C part of the electrical component. In the particular case of smart devices, the justification of smart devices for nuclear safety applications [Ref-2] addresses the concept of Production Excellence and Independent Confidence Building Measures.

A limited number of safety classified components will not be designed to the RCC-E code/IEC standards, but similar appropriate high standards will be adopted and justified by an ALARP analysis. Typically in such cases, a well-established design is available and trying to apply RCC-E/IEC standards would be counter-productive. An example could be a safety class 3 component of the conventional island, already designed for other nuclear and non-nuclear power plants.

When interfaces exist between a higher and a lower class I&C component, the component at the interface is designed in order to ensure that a failure will not propagate from a lower safety class component to higher safety classified components.

### **7.4.7. Quality Assurance**

#### **7.4.7.1. Quality Assurance during Construction**

Quality aspects cover all the activities of the construction of the product, i.e. design, engineering, machining, inspection and in-service testing. The application of a graded approach ensures a QA effort commensurate with the safety importance of the components as indicated by the safety class.

This graded approach is applied through three main aspects of the quality assurance: the quality management system applicable to the product (QMS), the surveillance of the product realisation, and the product documentation:

- safety class 1 and 2 require the implementation of a QMS which refers to the applicable nuclear quality,
- safety class 3 requires the implementation of a QMS which refers to industrial practice or potentially to applicable nuclear quality,
- for class NC there is no requirement to implement a specific QMS.

#### **7.4.7.2. In-service Quality Assurance**

The requirements with regard to in-service activities, referred to as Examination Maintenance, Inspection and Testing (EMIT), are detailed in a dedicated document (Sub-chapter 18.2).

The level of requirements is graded similarly to the grading of quality assurance during construction described above.

## **7.5. SUMMARY OF COMPONENT REQUIREMENTS**

The table below defines the component requirements

Component safety class	Robustness against LOOP	Robustness against earthquake	Qualification for accident conditions	Component Requirement	Design code	Level of quality
------------------------	-------------------------	-------------------------------	---------------------------------------	-----------------------	-------------	------------------

**Pressure retaining mechanical**

See section 7.4.3	Class 1	Assigned from SFG	M1	RCC-M1	Nuclear quality
			M2	RCC-M2 or equiv <sup>10</sup>	
			M3	RCC-M3	
	Class 2		M2	RCC-M2 or equiv <sup>10</sup>	Nuclear quality
			M3	RCC-M3	
	Class 3		M2	RCC-M2 or equiv <sup>10</sup>	Industrial or nuclear quality
			M3	RCC-M3 or equiv <sup>11</sup>	
			NR	HES <sup>12</sup>	

**Non-pressure retaining mechanical components**

See section 7.4.4	Class 1	Assigned from SFG	N/A	BTS	Nuclear quality
	Class 2		N/A	BTS	Nuclear quality
	Class 3		N/A	BTS	Industrial or nuclear quality

**Electrical and I&C components**

See section 7.4.5 & 7.4.6	Class 1	Assigned from SFG	C1	RCC-E + BTS	Nuclear quality
	Class 2		C2	RCC-E + BTS	Nuclear quality
	Class 3		C3	RCC-E + BTS	Industrial or nuclear quality

<sup>10</sup> ASME III with supplements or, KTA with supplements.

<sup>11</sup> Harmonised European standards (Compliant with PED) with supplements.

<sup>12</sup> Harmonised European standards (Compliant with PED).



## **8. CLASSIFICATION AND REQUIREMENTS APPLIED TO STRUCTURES**

NPP structures have a specific safety role: protecting safety classified components, people and the environment from the harmful effect of ionising radiations. NPP structures house and protect components that perform PLSF as described in section 3.2 although no explicit link is made between the PLSF and structures. Similarly, the SFG/safety feature classification process described in section 4 is not applied to structures.

The justification, definition of specific functions and classification rules for structures are given below and are only applicable to structures and are not relevant to SFGs, safety features or components which are described in section 2.1.

### **8.1. ROLE OF STRUCTURES AND SAFETY FUNCTIONS**

The different NPP structures have two main roles to:

1. Provide protection to components (reference to PLSF O1 and O2, see section 3.2);
  - house and support components in a suitable environment;
  - protect components against internal and external hazards;
  - protect redundant components via an adequate separation or by an adequate design.

As described in section 5.1.2, the protection of redundant components is ensured through the allocation of the SFG components in the building consistent with the physical separation requirements of the specific SFG.

2. Protect the general public, workers and the environment from normal and accident situation by providing a barrier to the release of radioactivity (reference to PLSF C3, C5 and C6, see section 3.2);
  - in conjunction with other components; or
  - in order to prevent the uncontrolled release of radioactivity to the environment.

### **8.2. SAFETY CLASSES APPLIED TO STRUCTURES**

The safety class and the associated requirements for a given structure are defined based on its functions and the consequence of its failure on:

- Safety classified components to deliver their safety function or
- Potential release of radioactive material.

Two safety classes are defined for structures as follows:

- Safety class 1 is assigned:
  - In general to structures whose function is to provide protection against external hazards (including earthquake conditions) for:
    - Safety class 1 or safety class 2 components involved in a first line of protection LLSF,
    - Safety classified components involved in another level of defence in depth, if their robustness against earthquake (SC1) is required,

An exception to this general rule is the turbine hall, which is assigned safety class 2, despite that this structure could house a very limited number of components which fall within the above criteria. In that case ALARP, arguments should justify appropriate measures to protect those components.

- To structures whose function is to provide a barrier to the release of radioactivity or house components with a barrier role,
- Safety class 2 is assigned:
  - In general as a minimum to structures whose function is to house or provide protection against external hazards for safety classified components,
  - To structures whose failure, if they were not classified, could impair the integrity of safety class 1 structures, or impair components whose robustness against earthquake (SC1) is required.

Applying those rules, the Reactor Building and Safeguards Buildings are assigned to safety class 1. The chimney stack on the Fuel Building roof (potential interaction with the Reactor Building, Fuel Building and Division 4 of Safeguards Buildings) and the Turbine Hall (potential interaction with Divisions 2 and 3 of Safeguards Buildings) are assigned to safety class 2.

### **8.3. STRUCTURE REQUIREMENTS**

#### **8.3.1. Definitions**

Two structural definitions are used in the specification of the requirements for structures:

- Main structures
- Other structures

The main structures of a building are those which fulfil the safety classified function and which contribute to the building structural behaviour.

The other structures of a building, in general, are located inside the building. These other structures are secondary parts of the structure (e.g. internal parts, removable parts<sup>13</sup>, etc.) whose failure shall not affect the main structure. These structures do not contribute directly to the structural behaviour of the main structure, but are designed for a specific purpose (e.g. biological shielding, handling trapdoors, etc.) and may also contribute to safety.

Other structures comprise a wide variety of structural types and materials such as stairs, platforms, reinforced concrete, precast slabs or walls, steelwork with various cladding, steel plates, polyethylene plates and composite structures.

When anchored or housed in a safety classified building, these structures are nevertheless considered as safety classified structures.

These structures are referred to as "other structures" in the following sections.

### 8.3.2. Robustness against Single Failure - Redundancy

Single failure considerations usually do not apply to structures (e.g. buildings). Reasoned engineering (high reliability) arguments are usually made to justify the avoidance of passive single failure, based on good standards of design, construction, inspection and maintenance.

In the particular case of aircraft crash hazard, as described in Sub-chapter 13.1, two means of protection are applied: a physical separation or a robust design to withstand the crash.

### 8.3.3. Physical Separation

The physical separation applied to a structure is consistent with the classified components it protects or houses. Therefore, if the protected components are subject to physical separation (i.e. require physical separation from other components) the associated structure will be designed to fulfil this function, either through appropriate location of the building or through the use of internal barriers within the building.

As described in section 5.1.2, physical separation is ensured through the allocation of the components in the buildings consistent with the physical separation requirements of the SFG, to which the components belong.

### 8.3.4. Robustness against Earthquake

As for components in section 7.1, a safety classified structure shall be robust against earthquake conditions consistent with:

- The components it protects or its intrinsic safety function during and following an earthquake,
- The consequences on classified structures or components of its failure if it were not robust against earthquake conditions.

SC1 and SC2 requirements defined for components in the introduction of section 7.1 also apply to structures, with the rules detailed below.

---

<sup>13</sup> Removable parts include: Removable concrete slabs and walls, Handling trapdoor, Neutron shielding barriers, Biological shielding barriers.

In general, for safety class 1 structures:

- The main structures must be seismically designed and constructed to SC1 requirements.
- Other structures which perform a fire partition role will be seismically designed to SC1.
- The other structures must be seismically designed to SC2 as far as necessary (see below).

For safety class 2 structures:

- The structures (main and other) must be seismically designed to SC2 as far as necessary (see below).

It is necessary to apply SC2 requirements to a building, a structure which itself is not required to remain robust against earthquake, but whose failure could have an unacceptable impact on a structure or a component with an SC1 requirement.

In particular, if the collapse of a structure/building can directly or indirectly have an unacceptable impact on an adjacent structure or component designed with an SC1 requirement (domino effect), this structure/building must be designed with an SC2 requirement. Unacceptable impact may also result from the internal hazards subsequent to an earthquake (see section 7.1).

In general, structures assigned SC1 requirements involve the definition of stability and component support integrity criteria.

**Stability** is the ability of a structure to resist loads which have a tendency to modify its position or orientation (for example, which have a tendency to cause the structure to tilt, fall or slide in an unacceptable manner or which could lead to a breakage of the structure). The stability of a structure relies upon the stability and resistance of its supports.

**Integrity of component supports** is the behavioural ability of a structural element of a larger structure, which supports a component in resisting seismic loads so that the component to be protected meets its requirements.

The loads due to postulated earthquake are defined in combination with the other loads to be considered in the design basis (see section 8.3.7).

Structures assigned SC2 requirements are designed using methods appropriate to their requirements. In general, structures assigned SC2 requirements involve the definition of stability criteria.

In general, an “other structure” does not support components directly but is itself required to be supported by a main structure. In this case, the requirements involve the definition of component support integrity criteria.

### 8.3.5. EMIT

Whilst there is a requirement for inspection and maintenance during the lifetime of a safety classified structure, some requirements must be defined in advance for the design and the loads applicable. In general, this is addressed through the application of design codes.

The detailed requirements are generally determined after the design has been established, as part of the site licensing detailed studies.

### 8.3.6. Structures Requirements

Associated with the safety classes, two safety requirement levels (C1, C2) are defined for Structures as follows:

- Safety class 1 structures must meet C1 requirements,
- Safety class 2 structures must meet C2 requirements;

### 8.3.7. Design Codes to be applied for Structures

For C1 structures: The main structures (e.g. the Reactor Building internal containment, foundation raft, etc.) must comply with the ETC-C design code.

For C2 structures: The main structures must comply with dedicated design rules provided in the definition of C2 safety requirements [Ref-1] and the civil works dedicated rules [Ref-2].

Due to their specific role, the C1 and C2 "other structures" such as shielding protection inside the Reactor Building may consist of steel plates, polyethylene plates, etc. for which ETC-C or the civil works dedicated rules [Ref-2] are not suitable (not specifically defined for this purpose), although it is used as a guideline to assist in the choice of design code to be applied and to define the requirements. For this reason, "other structures" are to be designed in accordance with dedicated rules.

Nevertheless, the anchorages of support of those C1 "other structures" shall comply with ETC-C.

C1 other structures such as stairs and platforms must comply with ETC-C design code requirements.

For C1 other structures, such as concrete structures or steelwork structures, the Licensee shall determine the relevant design code, with an assumption of a linear elastic material behaviour under seismic loading conditions, to be applied such as ETC-C design code or EN 1992 (concrete structures) or EN 1993 (steelwork structures).

In case of robustness to earthquake requirement (SC1 or SC2), the seismic detailed rules applied are:

- C1 and C2 main structures: ETC-C rules (this refers to the Seismic Detailing Rules for Safety Classified Structures [Ref-3]),
- C1 other structures such as stairs and platforms: ETC-C rules (this refers to the Seismic Detailing Rules for Safety Classified Structures [Ref-3])
- C1 other structures such as concrete structures: EN 1992,
- C1 other structures such as steelwork structures: EN 1993,
- C1 other structures (other than concrete/steel): dedicated rules consistent with European Standards applicable to this specific type of structure.

Other structures such as concrete slabs with SC1/SC2 requirements shall be designed with an assumption of a linear elastic material behaviour under seismic loading conditions, on the basis of ETC-C principles with specific additional rules.

The design requirements for classified structures are defined for different load combinations considered in the design basis, including loads due to postulated earthquake (in case of SC1/SC2 requirement - Sub-chapter 3.3). The requirements cover the following aspects:

- **Stability:** behavioural requirements whose purpose is to prevent the collapse of a structure.
- **Local stability:** behavioural requirements which are expressed in terms of static balance, mechanical resistance and rigidity.
- **Integrity of component supports:** behavioural requirements which describe the fact that the structural elements that support items of a component must meet the requirements attributed to the component.
- **Containment:** the aim of the containment function is to limit the release of hazardous materials into the environment.
- **Avoidance of interaction:** the aim is to prevent impacts between adjacent components (including structures) during earthquakes. Interactions occur when the relative displacement of the components is greater than the separation distance between them.

**8.4. SUMMARY OF SAFETY CLASSES AND REQUIREMENTS**

Safety class	Robustness against earthquake	EMIT	Structure requirement	Design codes and standards	Seismic detailed rules	
<b>Main structures</b>						
1	Yes (SC1)	Yes	C1 (main structures)	ETC-C <sup>16</sup>	ETC-C <sup>17</sup>	
2	As far as necessary (SC2 or no requirement)	Yes	C2 (main structures)	Dedicated rules [Ref-1] and [Ref-2]	ETC-C <sup>17</sup>	
<b>Other structures</b>						
See section 8.3	1	Yes (SC1)	C1 (stairs and platforms)	ETC-C <sup>16</sup>	ETC-C <sup>17</sup>	
	1	As far as necessary (SC2 or SC1 if fire partition function or no requirement)	As far as necessary (to be specified by the Licensee)	C1 (concrete structures)	ETC-C <sup>16</sup> or EN 1992 <sup>18</sup> (linear elastic calculation for seismic design)	EN 1992
				C1 (steelwork structures)	ETC-C <sup>16</sup> or EN 1993 <sup>14</sup> (linear elastic calculation for seismic design)	EN 1993
				C1 (other structures – other than concrete/steel)	Dedicated rules <sup>19</sup>	Dedicated rules <sup>15</sup>
	2	As far as necessary (SC2 or no requirement)	As far as necessary (to be specified by Licensee)	C2 (other structures)	Dedicated rules [Ref-1]	Dedicated rules <sup>15</sup>

Requirements “Robustness against Single Failure” and “Physical separation” are not included in the table since they are not considered to be significant for the structures as described in section 8.3.

<sup>16</sup> ETC-C refers to the AFCEN ETC-C 2010 accompanied by the UK Companion Document as described in Sub-chapter 3.8.

<sup>17</sup> Refers to [Ref-3]

<sup>18</sup> The choice of whether to specify ETC-C or the relevant Eurocode Standard lies with the Licensee.

<sup>19</sup> The dedicated rules which apply to non-steel/concrete “other C1 structures” are in line with the current European Standards corresponding to material of each specific structure.

## 9. CLASSIFICATION AND PSA FEEDBACK

For all plant SSCs, the definition and application of safety classification strategy is an iterative process, developed deterministically, and supplemented by probabilistic risk insights, resulting in a balanced classification scheme. Once the deterministic classification process has been applied, the resulting safety classification map is analysed, taking into account probabilistic risk insights, and overall SSC classifications. In practice, the risk insights are derived from the plant Probabilistic Safety Assessment (PSA), plant models of the protection functions necessary to mitigate the typical range of accidents and hazards.

It is important to note that the assignment of a SFG to safety class 1, as a result of the deterministic process, reflects the safety significance and results in the application of the highest level of quality assurance grade in terms of specification, design, procurement, installation and operation. The importance of applying probabilistic risk insights to SFGs deterministically assigned to safety class 1 is not considered to be as significant in comparison to SFGs assigned deterministically to safety class 2 or 3, as obviously a probabilistic review of deterministically assigned class 1 SFGs cannot result in a classification upgrade. Nevertheless, it is confirmed that the PSA review will be conducted on all safety classes. Where figures of lower than  $10^{-5}$  (pfd or frequency) are required, this should be considered as a strong indicator that a diverse back-up system is required.

The probabilistic review is therefore conducted on SFGs which are deterministically assigned to safety class 1, 2 and 3. The PSA team (who perform the probabilistic review) compares the reliability of the SFGs implemented in the PSA model, to reliability guidelines that have been determined by expert judgement. These guidelines are judged to be an acceptable range of reliability for a given SFG based on its deterministically assigned safety class. The range of reliability guidelines is given below (in terms of failures per demand) and potentially may lead to discussion or interpretation during the review process:

SFG class	Probability of failure on demand (pfd) <sup>20</sup>
Class 1	$10^{-5} \leq \text{pfd} \leq 10^{-3}$
Class 2	$10^{-3} < \text{pfd} \leq 10^{-2}$
Class 3	$10^{-2} < \text{pfd} \leq 10^{-1}$

In addition, the following table provides reliability guidelines for continuous acting or high demand systems (in terms of failure frequencies):

SFG class	Failure frequency/yr (ff) <sup>20</sup>
Class 1	$10^{-5} \leq \text{ff} \leq 10^{-3}$
Class 2	$10^{-3} < \text{ff} \leq 10^{-2}$
Class 3	$10^{-2} < \text{ff} \leq 10^{-1}$

<sup>20</sup> These figures apply at the SFG level as a review of the outcome of the deterministic classification process. For the design of I&C systems, dedicated figures shall apply as detailed in the safety principles applied to the UK EPR I&C architecture [Ref-1].



Note that the guidelines in the previous two tables apply to SFGs, but are not applicable to a SFG grouping only passive components (pipework, heat exchanger tube, etc.) covered by ASME/RCCM and other mechanical codes. Since structures do not belong to SFGs and are passive items covered by ETC-C and other design codes, these guidelines are not applicable to structures.

As previously stated, this PSA review is applicable to class 1, 2, and 3 SFGs; however, if a non-classified SFG is modelled in the PSA, then a similar PSA review will be performed.

If the reliability of the SFG derived from the PSA is less reliable than the reliability guidelines but the Target 8 (Frequency dose targets for accidents on an individual facility – any person off the site) and Target 9 (Total risk of 100 or more fatalities) are still met with this PSA derived reliability, this confirms that safety is not compromised and the initial (deterministically-derived) classification is confirmed and recorded as the final classification.

The PSA studies of Chapter 15 already ensure that a balanced design is achieved and ensure that the risk from the plant is not dominated by or particularly sensitive to one particular category of fault. As part of the PSA review, while analysing Target 8 and Target 9, this aspect will be confirmed.

Adequate justification of the acceptability of the PSA data (relevance of OPEX data, etc.) will be addressed during the detailed design phase.

If reliability of the SFG implemented in the PSA is more reliable than the reliability guidelines requirements, then an appropriate ALARP justification will be provided which would include one of the following activities:

- If the values are relatively close, SFGs reliability implemented in the PSA will need to be justified – specifically a justification that the OPEX data is sound and relevant regarding the detailed design.
- If there is a larger discrepancy between values, a sensitivity analysis should be performed to highlight the impact of considering the reliability guidelines in the PSA. According to the changes of risk resulting from the sensitivity analysis, the following decisions should be taken as follows:
  - Risk insignificant: the initial (deterministically-derived) classification is confirmed and recorded as the final classification.
  - Risk significant: considering absolute impact on Targets 8 and 9 of the SAPs [Ref-2] (see Sub-chapter 3.1 and Chapter 15), but considering also relative impact via Risk Increase Factor (RIF) or other appropriate importance measures, the preliminary safety class might be upgraded to reflect the real importance of the SFG under consideration.
  - If, for a given system, there are a significant number of instances where the PSA reliability data is better than the reliability guidelines, then it would be necessary to carry out a sensitivity study to assess in the same way (significance of potential impact on Targets as described above) the cumulative effect on risk.

Once this PSA review has been performed according to the process described here above, the application of the safety classification approach is finalised.

In the future, PSA refinements maybe necessary, but licensees would have to determine how best to adapt the PSA and apply any necessary plant modifications based on OPEX and ALARP considerations.

## 10. APPLICATION OF UK EPR CLASSIFICATION APPROACH

Full application of the UK EPR classification approach providing classification of safety feature groups, safety features, systems, components and structures will take place during the Nuclear Site Licensing (NSL) phase. Accordingly, for GDA the application of the UK EPR classification approach has been performed on a limited basis.

The following tables present, based on the classification principles presented in this sub-chapter, the classification of the main systems, safety features or components of the plant, with their associated design requirements and main design codes.

- Sub-chapter 3.2 - Table 1: Classification of main mechanical **components associated with their safety features**,
- Note that for those **safety features** which fulfil mitigating functions under PCC or RRC conditions, further information is given in the fault schedule presented in Sub-chapter 14.7.
- Sub-chapter 3.2 - Table 2: Classification of main electrical systems,
- Sub-chapter 3.2 - Table 3: Classification of I&C systems,
- Sub-chapter 3.2 - Table 4: Classification of main civil structures,
- Sub-chapter 3.2 - Table 5: List of “other structures” in the Reactor Building
- Sub-chapter 3.2 - Table 6: Classification of fuel handling and storage SSCs (mechanical parts)

These tables will need to be updated as part of the detailed studies in NSL phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 3.2
	CHAPTER 3: GENERAL DESIGN AND SAFETY ASPECTS	PAGE : 55 / 70
		Document ID.No. UKEPR-0002-032 Issue 04

### SUB-CHAPTER 3.2 - TABLE 1

#### Classification of main mechanical components associated to their safety features

Note 1: for those SSCs which fulfil mitigating functions under PCC or RRC conditions, further information (especially about the architecture requirements) is given in the fault schedule presented in Sub-chapter 14.7.

Note 2: as electromechanical components (valves, pumps) may have several safety classes addressing the mechanical or the electrical and I&C parts of the components, the safety class indicated corresponds to the highest safety class of safety features. It does not mean that the whole component is class 1. It addresses only the mechanical parts.

*For GDA, this table will only report the results of the studies performed on the RCV [CVCS] and ASG [EFWS] and the classification of support systems DVL [SBVSE], DEL [SCWS], DVLnew [SBVSE], DELnew [SCWS] at system level in accordance with section 4.1.5.*

ECS	Description	Safety classification		Design requirements		Mechanical design code
		Highest safety function category	highest safety class of SFG	Mechanical quality for pressure retaining components	Seismic	
DVL [SBVSE]	Ventilation and air-conditioning of electrical and I&C rooms (excluding main control room level)	A	1	N/A	SC1	Non-nuc. code
DEL [SCWS]	Chilled water production	A	1	N/A	SC1	Non-nuc. code
DVLnew [SBVSE]	Emergency back-up of ventilation and air-conditioning of electrical and I&C rooms (excluding main control room level)	A	1	N/A	SC1	Non-nuc. code
DELnew [SCWS]	Emergency back-up of chilled water production for cooling in electrical and I&C rooms	B	2	N/A	SC1	Non-nuc. code

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 3.2
	CHAPTER 3: GENERAL DESIGN AND SAFETY ASPECTS	PAGE : 56 / 70
		Document ID.No. UKEPR-0002-032 Issue 04

ECS	Description	Safety classification		Design requirements		Mechanical design code
		Highest safety function category	highest safety class of SFG	Mechanical quality for pressure retaining components	Seismic	
<b>ASG [EFWS]</b>	<b>Steam Generator Emergency FeedWater System</b>					
	<u>SF - Start-up of an ASG [EFWS] train</u>	A	1			
	Header from steam generator to and including isolation valves ASGi410VD	A	1	M2	SC1	RCC-M2
	Header at ASG [EFWS] pump discharge to isolation valves ASG1410VD, ASGi310VD, ASGi213VD, ASG520iVD	A	1	M3	SC1	RCC-M3
	Header at ASG [EFWS] pump suction to and including isolation valves ASGi103VD and ASG510iVD	A	1	M3	SC1	RCC-M3
	ASG [EFWS] Tank (ASG1110BA)	A	1	M3	SC1	RCC-M3
	ASG [EFWS] Pump (ASG1210-PO)	A	1	M3	SC1	RCC-M3
	<u>SF - ASG [EFWS] pump suction realignment</u>	B	2			
	ASG [EFWS] pump suction realignment common header (from isolation valves ASG5101VD (excluded) to and including ASGj302VD)	B	2	M3	SC1	RCC-M3
	<u>SF - ASG [EFWS] pump discharge realignment</u>	A	1			
	ASG [EFWS] pump discharge realignment common header (excluded isolation valves ASG520iVD)	A	1	M3	SC1	RCC-M3
	<u>SF - Replenishment of ASG [EFWS] tanks</u>	C	3			
ASG [EFWS] tank replenishment header (from isolation valves ASGj302VD (excluded) to and including isolation valves ASGj211VD and ASGj402VD)	C	3	NC	SC1	Non-nuc. code	
ASG [EFWS] replenishment pump ASGj210PO	C	3	NC	SC1	Non-nuc. code	

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 3.2
	CHAPTER 3: GENERAL DESIGN AND SAFETY ASPECTS	PAGE : 57 / 70
		Document ID.No. UKEPR-0002-032 Issue 04

ECS	Description	Safety classification		Design requirements		Mechanical design code
		Highest safety function category	highest safety class of SFG	Mechanical quality for pressure retaining components	Seismic	
<b>RCV [CVCS]</b>	<b>Chemical and volume control system</b>					
	<u>SF-Control of core boron concentration in normal operation</u>	C	3			
	HP charging pumps	C	3	M3	SC2	Non-nuc. code
	<u>SF-Boration after the non-hazardous stable state of design basis event is reached</u>	C	3			
	HP charging pumps	C	3	M3	SC2	Non-nuc. code
	<u>SF-Isolation downstream of volume control tank and hydrogenation station</u>	A	1			
	Isolation valves downstream Volume Control Tank	A	1	M3	SC1	Nuclear code
	<u>SF-RCP Seal Water Injection</u>	C	3			
	HP charging pumps	C	3	M3	SC2	Non-nuc. code
	Seal injection and leak off filters	C	3	M3	NC	Non-nuc. code
	<u>SF-Charging pumps suction switchover to IRWST</u>	A	2			
	IRWST – RCV [CVCS] connection lines and isolation valves	A	2	M3	SC2	Nuclear code
	<u>SF-RCS pressure reduction by auxiliary spray</u>	C	3			
	HP charging pumps	C	3	M3	SC2	Non-nuc. code
	Three-way valve to PRZ auxiliary spray	C	3	M3	SC2	Non-nuc. code
Auxiliary spray line motorized isolation valve	A	1	M3	SC1	Nuclear code	
Auxiliary spray line isolation check valve	A	1	M1	SC1	Nuclear code	

ECS	Description	Safety classification		Design requirements		Mechanical design code
		Highest safety function category	highest safety class of SFG	Mechanical quality for pressure retaining components	Seismic	
	<u>SF-Adjustment of the letdown flow</u>	B	2			
	HP reducing stations	B	2	M3	SC2	Nuclear code
	LP reducing station	A	1	M2	SC1	Nuclear code
	<u>SF-HP Letdown isolation by means of isolation valves downstream HP reducing stations</u>	C	3			
	Isolation valves downstream HP reducing stations	C	3	M3	SC1	Nuclear code
	<u>SF-LP Letdown isolation</u>	A	1			
	RCV [CVCS] LP letdown line via Safety Injection System [RIS], including LP reducing station and downstream isolation valve	A	1	M2	SC1	Nuclear code
	<u>SF-Integrity of RCPB up to CVCS 2nd Isolation Valve</u>	A	1			
	RCV [CVCS] HP letdown line, from the primary loop down to and including the 2nd isolation valve	A	1	M1	SC1	Nuclear code
	Charging line, from the primary loops [RCPB] to the 2nd RCV [CVCS] isolation valve &	A	1	M1	SC1	Nuclear code
	Auxiliary spray line from the 1st isolation valve (RCP [RCS]) to the 2nd isolation valve (RCV [CVCS])	A	1	M1	SC1	Nuclear code
	<u>SF-RCPB Isolation in accident conditions</u>	A	1			
	RCV [CVCS] HP letdown line, from the primary loop down to and including the 2nd isolation valve	A	1	M1	SC1	Nuclear code
	Charging line, from the primary loops [RCPB] to the 2nd RCV [CVCS] isolation valve &	A	1	M1	SC1	Nuclear code

ECS	Description	Safety classification		Design requirements		Mechanical design code
		Highest safety function category	highest safety class of SFG	Mechanical quality for pressure retaining components	Seismic	
	Auxiliary spray line from the 1st isolation valve (RCP [RCS]) to the 2nd isolation valve (RCV [CVCS])	A	1	M1	SC1	Nuclear code
	Containment isolation	A	1			
	Containment penetrations (charging, letdown, RCP seals injection and return) and associated isolation devices	A	1	M2	SC1	Nuclear code
	<u>SF-Integrity of RCV parts associated with RRI [CCWS] cooling chain for safety users</u>	B	2			
	HP Coolers and lines connected to RRI	B	2	M3	SC1	Nuclear code
	<u>SF-CVCS pressure boundaries downstream 2nd isolation valve</u>	C	3			
	Regenerative heat exchanger	C	3	M3	SC2	Non-nuc. code
	HP Coolers	C	3	M3	SC2	Non-nuc. code
	Coolant purification cartridge filters	C	3	M3	NC	Non-nuc. code
	Demineralizers	C	3	M3	NC	Non-nuc. code
	Volume Control Tank	C	3	M3	SC2	Non-nuc. code
	HP charging pumps	C	3	M3	SC2	Non-nuc. code

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 3.2
	CHAPTER 3: GENERAL DESIGN AND SAFETY ASPECTS	PAGE : 60 / 70
		Document ID.No. UKEPR-0002-032 Issue 04

### SUB-CHAPTER 3.2 - TABLE 2

#### Classification of main electrical systems

ECS	Description	Safety class	Seismic requirement
LHA/B/C/D	10 kV emergency power supply system	1	SC1
LJA/B/C/D/F/G/H/I	690 V emergency power supply system	1	SC1
LLU/X	400 V emergency power supply system	2	SC1
LJZ	690V emergency power supply system, third PTR pump	2	SC1
LJP/S	690 V Ultimate diesel generator (UDG) sets division 1/4	2	SC1
LLA/B/C/D/P/Q/R/S	400 V emergency power supply system	1	SC1
LLF/G/H/I	400 V emergency power supply system (LH diesel auxiliaries)	1	SC1
LHP/Q/R/S	10 kV emergency diesel generator (EDG) units division 1/2/3/4	1	SC1
LOA/B/C/D/F/G/H/I	400V regulated power supply system	1	SC1
LVA/B/C/D/F/G/H/I	400V 2 hours uninterrupted power supply system	1	SC1
LVP/S	400V 12 hours uninterrupted power supply system	2	SC2
LAA/B/C/D	220 V DC 2 hours uninterrupted power supply system	1	SC1
LGF/G/H/I	10 kV normal power supply system	3	SC2
LIF/I	690 V normal power supply system	3	SC2
LKK/L/M/N/P.Q/R/S	400 V normal power supply system	3	SC2
LTR	Earth circuit	1	SC2
DN	Normal lighting for building and open areas of site	NC	SC2
DS	Emergency lighting for building and open areas of site	3	SC1
All other switchboards		NC	NR



**SUB-CHAPTER 3.2 - TABLE 3**

**Classification of I&C systems**

<b>I&amp;C system</b>	<b>Safety classification</b>	<b>Seismic requirement</b>
<b>RPR [PS] – Reactor protection system (*)</b>	1	SC1
<b>RCSL – Reactor Control, Surveillance and Limitation System</b>	2	NC (**)
<b>PAS – Process control system</b>	3	SC2
<b>SAS – Safety automation system</b>	2	SC1
<b>RRC-B SAS – RRC-B Safety Automation System</b>	3	SC1
<b>SA I&amp;C – Severe Accident I&amp;C system</b>	3	SC1
<b>MCS [SICS] – Safety information and control</b>	1	SC1
<b>MCP [PICS] – Process information and control</b>	3	SC1
<b>NCSS – Non-Computerised safety system</b>	2 (***)	SC2 (****)

- (\*) The PSOT interface is part of RPR [PS] system.
- (\*\*) As a system used in normal operation and whose failure in a seismic event has no unacceptable impact on SC1 equipment
- (\*\*\*) In accordance with section 5.2.4, NCSS contributes to a category C function of a risk reduction line (backup line) and should be assigned to safety class 3, but is safety class 2 due to its reliability claim.
- (\*\*\*\*) In accordance with section 7.1.2 a requirement of robustness against earthquake SC2 is assigned in order to ensure that a failure would not have an unacceptable impact on SC1 components.



Description	Civil structure classification	Requirements	Seismic requirement	Protection from aircraft crashes	Protection from external explosion
<b>Fuel buildings (FB)</b> - Structures i.e. metal liners (spent fuel pool, transfer compartment), metal parts embedded in the concrete - Other structures and components	1	C1		Yes	Yes
<b>Diesel generator buildings</b> - Structures - Other structures and components	1	C1	SC1 SC2	No <sup>(2)</sup>	Yes
<b>Pumping station</b> - Structures, i.e. water intake structure from the pumping station and pipes connected to class 1 seismic buildings - Other structures and components	1	C1	SC1 SC2	Yes (3)	Yes
<b>Effluent treatment building (ETB)</b>	1	C1	SC1	No	Yes
<b>Nuclear Auxiliary Building stack</b>	2	C2	SC2	No	Yes
<b>Turbine hall</b>	2	C2	SC2	No	No
<b>Nuclear Auxiliary Building /Effluent Treatment Building tunnel</b>	1	C1	SC1	No	No
<b>SEC [ESWS] galleries</b>	1	C1	SC1	No (1)	No
<b>Electrical Building access tower</b>	2	C2	SC2	No	Yes

- (1) Protecting the Nuclear Auxiliary Building must take into account radioactive discharge risks.  
 (2) Protecting diesel generator buildings from aircraft crashes is ensured by physical separation  
 (3) by physical separation or aircraft shell

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 3.2
	CHAPTER 3: GENERAL DESIGN AND SAFETY ASPECTS	PAGE : 64 / 70
		Document ID.No. UKEPR-0002-032 Issue 04

### SUB-CHAPTER 3.2 - TABLE 5

#### List of “other structures” in the Reactor Building and associated design requirements

The previous table is removed as it is not applicable to UK GDA EPR.

The identification of C1 ‘Other Structures’ (Removal Parts) [Ref-1] lists the safety class 1 structures in NI buildings (Reactor Building – Fuel Building – Safeguard Buildings), that are classified as “other structures” (removable parts)

### SUB-CHAPTER 3.2 - TABLE 6

#### Classification of fuel handling and storage SSCs (mechanical parts)

Description of the mechanical handling devices (mechanical parts only)	Safety class	Applicable Codes and standards and/or requirements		Seismic requirements	Quality assurance
		KTA	BTS		
Spent fuel mast bridge	2	Requirements for spent fuel mast bridge	HS Level 2	SC2	Yes
Spent fuel cask transfer facility (DMK) <sup>(1)</sup> (Specific parts of the spent fuel cask transfer machine, including the structure, travel and direction drives, travel guides, cask upper trunnion clamping system and anti-seismic locking devices)	2	Additional requirements	HS Level 2	SC1	Yes
Polar crane main hoist	1	Not applicable	HS Level 1	SC2	Yes
Polar crane secondary hoist	1	Not applicable	HS Level 1	SC2	Yes
Polar crane auxiliary hoist	1	Not applicable	HS Level 1	SC2	Yes
Spent fuel handling tool	2	Additional requirements	HS Level 2	SC2	Yes
Spent fuel examination facility	3	Non-classified	Non-classified	SC2	Yes

## **SUB-CHAPTER 3.2 – REFERENCES**

External references are identified within this sub-chapter by the text [Ref-1], [Ref-2], etc at the appropriate point within the sub-chapter. These references are listed here under the heading of the section or sub-section in which they are quoted.

### **1. PURPOSE OF CLASSIFICATION – APPROACH FOLLOWED**

**[Ref-1]** Classification of structures, systems and components. NEPS-F DC 557 Revision D. AREVA NP. October 2012. (E)

### **2. OVERVIEW OF THE CLASSIFICATION METHODOLOGY**

#### **2.1. DEFINITIONS**

**[Ref-1]** IAEA Safety Glossary. Terminology Used in Nuclear Safety and Radiation Protection. ISBN 92-0-100707-8. 2007 Edition. (E)

**[Ref-2]** IAEA Safety Standards – Safety Classification of Structures, Systems and Components in Nuclear Power Plants. Draft Safety Guide DS367. Draft 6.3. June 2012. (E)

**[Ref-3]** IAEA Safety Standards - Safety of Nuclear Power Plants: Design. NS-R-1. 2000. (E)

**[Ref-4]** Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

**[Ref-5]** Safety principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

**[Ref-6]** UK Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. January 2008. (E)

#### **2.2. BACKGROUND**

**[Ref-1]** IAEA Safety Standards - Safety of Nuclear Power Plants: Design. NS-R-1. 2000. (E)

**[Ref-2]** IAEA Safety Standards – Safety Classification of Structures, Systems and Components in Nuclear Power Plants. Draft Safety Guide DS367. Draft 6.3. June 2012. (E)

**[Ref-3]** Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

**[Ref-4]** UK Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. January 2008. (E)

### **2.2.1. Safety Assessment Principles**

[Ref-1] UK Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. January 2008. (E)

### **2.2.2. IAEA Standards – NS-R-1 and DS367**

[Ref-1] IAEA Safety Standards - Safety of Nuclear Power Plants: Design. NS-R-1. 2000. (E)

[Ref-2] IAEA Safety Standards – Safety Classification of Structures, Systems and Components in Nuclear Power Plants. Draft Safety Guide DS367. Draft 6.3. June 2012. (E)

### **2.2.3. IEC Standards – IEC 61226 and IEC 61513**

[Ref-1] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

[Ref-2] Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems. IEC 61513. Edition 2001. (E)

## **2.4. ALARP PRINCIPLES AND CLASSIFICATION**

[Ref-1] UK Health and Safety Executive (HSE). Technical Assessment Guide, ND Guidance on the Demonstration of ALARP (As Low As is Reasonably Practicable). T/AST/005 Issue 4. January 2009. (E)

[Ref-2] F. Romanet. UK EPR ALARP methodology to support the design modification process. ENSNDR100088 Revision A. EDF/SEPTEN. July 2010. (E)

## **3. SAFETY FUNCTION DEFINITION AND CATEGORISATION**

### **3.1. DERIVATION OF SAFETY FUNCTIONS**

[Ref-1] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

### **3.2. DEFINITION OF PLANT LEVEL SAFETY FUNCTIONS (PLSF)**

[Ref-1] IAEA Safety Standards - Safety of Nuclear Power Plants: Design. NS-R-1. 2000. (E)

### **3.3. DEFINITION OF LOWER LEVEL SAFETY FUNCTIONS (LLSF)**

[Ref-1] Safety principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

### **3.4. LOWER LEVEL SAFETY FUNCTION CATEGORISATION**

[Ref-1] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

[Ref-2] UK Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. January 2008. (E)

#### **3.4.1. Category A**

[Ref-1] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

#### **3.4.2. Category B**

[Ref-1] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

#### **3.4.3. Category C**

[Ref-1] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. BS IEC 61226:2009. (E)

## **4. CLASSIFICATION**

### **4.3. SAFETY CLASSES APPLIED TO SAFETY FEATURE GROUPS, SAFETY FEATURES AND COMPONENTS**

#### **4.3.1. Introduction**

[Ref-1] IAEA Safety Standards – Safety Classification of Structures, Systems and Components in Nuclear Power Plants. Draft Safety Guide DS367. Draft 6.3. June 2012. (E)

## **5. ARCHITECTURE REQUIREMENTS APPLIED TO SAFETY FEATURE GROUPS**

### **5.1. DEFINITION OF THE ARCHITECTURE REQUIREMENTS**

#### **5.1.1. Robustness against Single Failure and Redundancy**

[Ref-1] IAEA Safety Standards - Safety of Nuclear Power Plants: Design. NS-R-1. 2000. (E)



## **7. REQUIREMENTS APPLIED TO COMPONENTS**

### **7.4. COMPONENT REQUIREMENTS**

#### **7.4.6. I&C Component Requirements**

[Ref-1] Safety principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

[Ref-2] Justification of smart devices for nuclear safety applications. ENSECC110102 Revision B. EDF. May 2012. (E)

[Ref-3] UK EPR Guideline for Application of Production Excellence and Independent Confidence Building. ECECC111134 Revision C. EDF. July 2012. (E)

## **8. CLASSIFICATION AND REQUIREMENTS APPLIED TO STRUCTURES**

### **8.3. STRUCTURE REQUIREMENTS**

#### **8.3.7. Design Codes to be applied for Civil Structures**

[Ref-1] UK EPR - Safety Class 2 structures – definition of C2 safety requirements. ENSN110130 Revision A. EDF. January 2012. (E)

[Ref-2] Civil works dedicated rules for buildings classified C2 “main structures”. ENGSGC110254 Revision B. EDF. June 2012. (E)

[Ref-3] UK EPR – GDA – Good Practice - Seismic Detailing Rules for Safety Classified Reinforced Concrete and Steel Structures. ENGSGC110157 Revision B. EDF. April 2012. (E)

### **8.4. SUMMARY OF SAFETY CLASSES AND REQUIREMENTS**

[Ref-1] UK EPR - Safety Class 2 structures – definition of C2 safety requirements. ENSN110130 Revision A. EDF. January 2012. (E)

[Ref-2] Civil works dedicated rules for buildings classified C2 “main structures”. ENGSGC110254 Revision B. EDF. June 2012. (E)

[Ref-3] UK EPR – GDA – Good Practice - Seismic Detailing Rules for Safety Classified Reinforced Concrete and Steel Structures. ENGSGC110157 Revision B. EDF. April 2012. (E)

## 9. CLASSIFICATION AND PSA FEEDBACK

**[Ref-1]** Safety principles applied to the UK EPR I&C architecture in terms of the requirements for diversity and independence. PEPS-F DC 90 Revision C. AREVA. August 2012. (E)

**[Ref-2]** UK Health and Safety Executive (HSE). Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. January 2008. (E)

### SUB-CHAPTER 3.2 - TABLE 5

**[Ref-1]** UK EPR – GDA – Identification of C1 ‘Other Structures’ (Removal Parts). ECEIG112228 Revision A. EDF. February 2012. (E)