Form10/00

UK ABWR

HITACHI

Document ID	:	GA91-9101-0101-05000
Document Number	:	XE-GD-0645
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 5 : General Design Aspects

Hitachi-GE Nuclear Energy, Ltd.

DISCLAIMERS

Proprietary Information

This document contains proprietary information of Hitachi-GE Nuclear Energy, Ltd. (Hitachi-GE), its suppliers and subcontractors. This document and the information it contains shall not, in whole or in part, be used for any purpose other than for the Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR. This notice shall be included on any complete or partial reproduction of this document or the information it contains.

Copyright

Table of Contents

Executive Summary

Unlike most Generic Pre-Construction Safety Report (PCSR) chapters, this chapter does not consider any specific topic area. Instead, it describes the high level generic approaches to nuclear safety that have been applied to various design aspects of the UK Advanced Boiling Water Reactor (ABWR). These generic approaches are prescribed in order to produce a generic safety case that is complete and consistent. Most importantly, the systematic application of these generic approaches seeks to provide a robust basis for demonstrating the overarching safety case claims made in Generic PCSR Chapter 1: Introduction, that 'A UK ABWR constructed on a generic site within the United Kingdom, meets all safety targets for the public, workers and the environment, and satisfies the principle that all risks are As Low As Reasonably Practicable (ALARP) for all operating and fault conditions.'

These generic approaches conform to the Nuclear Safety and Environmental Design Principles (NSEDP). The NSEDPs provide a framework for production of a safety case that meets UK expectations for a modern nuclear power plant safety case. Evidence of compliance of the UK ABWR design with the NSEDPs is presented throughout the Generic PCSR, and is summarised in an NSEDP compliance report.

This chapter provides a list of five Fundamental Safety Functions that must be met by the UK ABWR at all times to maintain nuclear safety. It breaks these down into sets of High Level Safety Functions (HLSFs), and explains how each Safety Functional Claim (SFC) made in the Generic PCSR is linked to one of these HLSFs. The principle of how SFCs and Safety Property Claims (SPCs) made on Structures, Systems and Components (SSCs) provide a basis for building a comprehensive and coherent safety case that is compliant with the NSEDPs is described. The principles used in the categorisation of Safety Functions and safety classification of SSCs that deliver those safety functions are also presented.

Definitions are presented of the different modes of operation, physical states and aspects of the UK ABWR that require consideration in the safety case. These include various Operating Stages in the ABWR lifecycle (e.g. construction, commissioning, operation and decommissioning), and various Reactor Operating Modes (e.g. power operation, shutdown, refuelling, etc.).

Specific SFCs, SPCs and safety classification for SSCs that conform to the principles described in this chapter are identified in many other Generic PCSR chapters, in particular the systems chapters. The modelling of faults in Generic PCSR analysis chapters (24: Design Basis Analysis, 25: Probabilistic Safety Assessment and 26:Beyond Design Basis and Severe Accident Analysis) then represents conditions, and makes assumptions, that are fully consistent with these specific SFCs and SPCs, taking account of the classification of the SSCs, and considering all of the Reactor Operating Modes.

The criteria by which faults are designated to be either within the Design Basis or Beyond Design Basis are presented, as well as the division of Design Basis faults into frequent or infrequent faults. These influence the specific acceptance criteria that are applied in analysis chapters for specific faults.

The chapter also describes the generic approaches to seismic categorisation, equipment qualification, the use of codes and standards, and the design approach to examination, maintenance, inspection and testing for SSCs. Application of these generic approaches to specific SSCs are described in the systems chapters of the Generic PCSR.

Since the specific applications of the generic principles presented in this chapter are described in other Generic PCSR chapters that have their own conclusions, there are no requirements for any conclusions to this generic chapter.

5.1 Introduction

Chapter 5 presents the general approach to design and outlines high level design principles and definitions based on the Nuclear Safety and Environmental Design Principles (NSEDP) [Ref 5.1-1]. These are used throughout the safety case described in the Generic PCSR. Documenting key high level principles and definitions separately in this Chapter aims to avoid unnecessary repetition in the Generic PCSR documentation and to ensure that these principles and definitions are used consistently throughout the safety case.

5.1.1 Background

The design of UK ABWR is based on the NSEDPs [Ref 5.1-1] which have been used in the development of UK ABWR. The NSEDPs reflect UK and international Good Practice and aim to ensure nuclear safety and environmental protection are fully addressed in the UK ABWR design and will therefore enable safe operation of the UK ABWR. The NSEDPs are also consistent with ONR Safety Assessment Principles (SAPs) [Ref 5.1-2].

5.1.2 Document Structure

The following sections are included in this chapter:

Section 5.2 Purpose and Scope:
This section gives the purpose and scope of the chapter.

Section 5.3 General Safety Design Bases:
This section describes key high level design principles and the outlines the general approach that the UK ABWR has taken in the development of UK ABWR GDA safety cases.

Section 5.4 Definition of Operating Stages, Modes and Conditions:
This section sets out definitions of operational stages from planning, through commercial operation to decommissioning, operating modes and plant operating conditions that are used in the Generic PCSR.

Section 5.5 Definition of Design Basis Faults and Beyond Design Basis Faults:
This section defines categories of fault and other abnormal conditions that are used in fault studies.

Section 5.6 Categorisation of Safety Functions and Classification of Structures, Systems and Components (SSCs):
This section lists High Level Safety Functions and describes the approach adopted to categorise safety functions and classify the SSCs that provide them. The section also gives specific classifications for structural items and includes requirements on SSCs during and after seismic events.

Section 5.7 Qualification of SSCs
This section describes the qualification approach for SSCs corresponding to their classification and the operating conditions under which they are required to operate.

Section 5.8 Applied Regulations, Codes and Standards

This section describes the approach to the application of appropriate regulations, codes and standards to SSCs depending on their safety function and classification.

Section 5.9 Examination, Maintenance, Inspection and Testing
This section describes the approach to examination, maintenance, inspection and testing (EMIT) to be carried out for SSCs depending on their safety function and classification to ensure that the required safety and reliability will be achieved throughout the plant life cycle and design life.

Section 5.10 - Conclusions.

In the design of UK ABWR, operational experience (OPEX) is considered to improve the plant. The procedure used to incorporate OPEX is shown in the OPEX Report for UK ABWR [Ref 5.1-3] and a high-level description of how OPEX has been used in the development of the ABWR design from earlier BWR designs is given in Generic PCSR Chapter 28: ALARP Evaluation.

This chapter is supported by a number of Topic Reports:

- List of Safety Category and Class for UK ABWR (AE-GD-0224) [Ref 5.1-4]
- Topic Report on Acts, Regulations, Codes and Standards (QGI-GD-0014) [Ref 5.1-5]
- Topic Report on Fault Assessment (UE-GD-0071) [Ref 5.1-6]
- Topic Report on Safety Requirements for Mechanical SSCs (SE-GD-0308) [Ref 5.1-7], and
- Other reports directly referenced in this chapter.

5.2 Purpose and Scope

5.2.1 Purpose

The purpose of Chapter 5 is to set out some general definitions, design conditions and principles, based on the NSEDPs, for consistent use throughout the safety case.
These definitions, conditions and principles are summarised as follows:

- Operational stages (planning, through commercial operation to decommissioning).
- Operating modes (start-up, power operation, refuelling, etc.).
- Operating conditions (normal operating conditions, fault conditions).
- Categories of fault and other abnormal conditions.
- High Level Safety Functions.
- Categorisation of safety functions.
- Classification of Structures, Systems and Components (SSCs).
- Qualification required for SSCs corresponding to their classification and the operating conditions under which they are required to operate.
- High-level regulations, codes and standards to be applied to SSCs depending on their safety function and classification, and
- Examination, maintenance, inspection and testing (EMIT) to be carried out for SSCs depending on their safety function and classification.

5.2.2 Scope

The chapter sets out general definitions, design conditions and principles that are applied everywhere in the safety case and throughout the Generic PCSR.
Environmental and security aspects of the UK ABWR design are covered in the Generic Environmental Permit (GEP) and Conceptual Security Arrangements (CSA) respectively. For links to GEP and CSA documentation please see Generic PCSR Chapter 1: Introduction. For GEP, where specific references are required, for example in Radioactive Waste Management, Radiation Protection and Decommissioning, these are included in the specific sections within the Generic PCSR.

5.3 General Safety Design Bases

5.3.1 Introduction

This section describes key high level design principles and outlines the general approach taken in development of the UK ABWR GDA safety cases. This includes the definition of the three key categories of claims that are used in GDA safety cases to ensure the safety case is presented in a clear and coherent manner using a Claims - Argument – Evidence (CAE) scheme as described in Generic PCSR Chapter 1: Introduction. The key categories of the Claims within GDA safety cases are Safety Functional Claims (SFCs), Safety Properties Claims (SPCs) and Human Based Safety Claims (HBSCs) (refer to the Safety Case Development Manual (SCDM) [Ref-5.6-4] Section 3 for details).

5.3.2 Safety Functions and definition of Safety Functional Claims

Section 5.6 (Categorisation and Classification of Structures, Systems and Components (SSCs)) defines the safety functions that are required to ensure that the ABWR design meets the relevant safety requirements. These functions are derived from the following Fundamental Safety Functions (FSFs):

FSF 1 - Control of reactivity
FSF 2 - Fuel cooling,
FSF 3 - Long term heat removal
FSF 4 - Confinement/Containment of radioactive materials, and
FSF 5 - Others

These FSFs are broken down into a set of High Level Safety Functions (HLSFs). The HLSFs define lower level safety functions which enable individual safety measures to be identified such that they contribute to the achievement of the overarching FSFs. The full list of HLSFs is defined in Section 5.6 (Categorisation and Classification of Structures, Systems and Components (SSCs))' and the corresponding topic report on List of Safety Category and Class for UK ABWR (see [Ref 5.1-4]).

HLSFs may be further decomposed into Safety Functional Claims (SFCs) specific to particular safety measures. SFCs are uniquely identified using the HLSF and the system code. The approach to linking HLSFs with functions delivered by corresponding safety measures is illustrated in the SCDM [Ref 5.6-4] Section 3 Figure 15 'Application of Safety Functional Claims (SFCs) and Safety Property Claims (SPCs) in GDA documentation'.

5.3.3 Fundamental Design Principles

The Nuclear Safety and Environmental Design Principles (NSEDPs) [Ref 5.1-1] set down the fundamental bases for nuclear safety, non-radiological and radiological environmental protection that are applied in the UK ABWR design. The NSEDPs are the equivalent of SAPs in the UK

regulatory scheme. The SAPs are intended for use by ONR to confirm that the design meets the relevant regulatory expectations. Hitachi-GE has developed NSEDPs to form a framework of acceptance criteria by which the adequacy of the generic design is judged in order to ensure that the risks arising from all aspects of UK ABWR lifecycle are reduced to a level that is As Low As Reasonably Practicable (ALARP).

5.3.4 Safety Functional Claims (SFCs) and Safety Property Claims (SPCs)

- Safety Functional Claims (SFCs): SFCs are derived directly from the high level safety functions (HLSFs) that themselves are derived from the wide ranging and comprehensive fault analysis (Design Basis Analysis (DBA), Beyond Design Basis Analysis (BDBA), Severe Accident Analysis (SAA) and Probabilistic Safety Analysis (PSA)). There is a direct relationship between the HLSFs and the SFCs and it is the SFCs that are used to link safety claims to an appropriate Structure, System or Component (SSC). The key point of SFCs is that all systems that either perform the safety function or provide support (power, cooling chain, Control and Instrumentation (C&I) etc.) use the same HLSF within the SFC code. This means that each SFC code is both unique but also self-referencing across engineering disciplines and can be readily traced back to the fault studies from where the requirements for SFCs are derived. Consistency is achieved by using unique numbers throughout. SFCs are actions performed by an SSC to directly implement the safety function, for example insert control rods, open a valve, start a pump etc. SFCs for support systems are directly linked to the provision of for example, energy, cooling and initiation signal from C&I etc. to directly support actions such as, for example, starting the high pressure core flooder. In passive systems, such as metal and civil structures, SFCs are directly related to the key integrity functions to ensure a robust structural design.

- Safety Property Claims (SPCs): SPCs are those claims that provide the safety justification that the UK ABWR is compliant with Hitachi-GE's NSEDPs [Ref 5.1-1] and covers matters such as the integrity, reliability and environmental qualification for the claimed SSC. SPCs provide a safety justification of the major properties an SSC or its essential support system (ESS) has to have in order to discharge their safety functional claims. SPCs do not use an HLSF number as part their numbering but are assigned unique numbers within the relevant topic areas. The reason for is that many SSCs and ESS have to fulfil multiple SFCs whereas the SPCs are unique to the SSC.

Claims are closely aligned to and become requirements in the engineering specifications for the SSCs and ESS. Requirements specifications are often subdivided into, for safety matters, Safety Functional Requirements (SFRs) and Non-Functional Safety Requirements (NFSRs). For the Claims, Arguments and Evidence (CAE) used in this Generic PCSR the SFRs directly relate to SFCs and the NFSRs are related to SPCs.

The following provides a brief explanation of the SFC and SPC numbering system to help with the understanding of the claims tables in appendices A and B of many of the remaining chapters of this Generic PCSR.

SFCs are directly and uniquely linked to the HLSFs through the HLSF number and this number is used in the top claim and all claims. Traceability of the SFCs to the fault analysis is enabled by ensuring that all fault sequence analysis quotes the relevant HLSF number, a good example taken from the fault schedule is shown below:

RPS scram "APRM simulated thermal power high" (A1, Ω, **1-3**)

The above shows the HLSF number in bold, where HLSF **1-3** is the safety function 'Emergency Shutdown of the Reactor', A1 is the functional category and class and the Greek capital letter Ω means automatic initiation (it would be Greek capital letter Σ for manual initiation). This number is used in all relevant SFCs and is hence self-referencing to the Fault Schedule. The above example is taken from the Fault Schedule; a similar identification scheme is used for BDBA and SAA.

The SFC number takes the form:

(SSC identifier) SFC (HLSF number).(SFC number)

e.g**. RHR SFC 2-1.1**

So for example HLSF 2-1 is for functions to cool the reactor. So, considering the example of the Residual Heat Removal System (RHR), the top level safety functional claim would be numbered:

RHR SFC 2-1.1

through the following claim: 'The RHR through its Low Pressure Flooder System (LPFL) mode is a principal means to provide reactor core cooling as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of LOCA. This function is categorised as Category A and the components to deliver it are
designed to meet Class 1 requirements.

In a number of occasions, especially support systems, the functions are delivered through a subsystem. To help establish an audit trail of the CAE, a top claim assigned to the subsystem can be

defined. This is then broken down into claims that are assigned to the specific supported SSCs or SSCs delivering the corresponding function.

For example HLSF 2-1 is for functions to cool the reactor. A good example of a support system is for functions to cool the reactor is the Safety System Logic and Control System (SSLC), the top level safety functional claim is numbered as follows:

SSLC SFC 2-1.1:

SSLC provides the functions to control the systems assigned as the first provision for the Category A Safety Function to cool the reactor core. Claims are then made on the subsystems Reactor Core Isolation Cooling System (RCIC), High Pressure Core Flooding System (HPCF), Automatic Depressurisation System (ADS) and Low Pressure Flooder System (LPFL) / Residual Heat Removal System (RHR) all of which are actuated by the SSLC. A typical numbering scheme for these subsystems is then as follows:

SSLC SFC 2-1.1.1 (safety functional claim on the actuation of the RCIC)
SSLC SFC 2-1.1.2 (safety functional claim on the actuation of the HPCF)
SSLC SFC 2-1.1.3 (safety functional claim on the actuation of the ADS)
SSLC SFC 2-1.1.4 (safety functional claim on the actuation of the LPFL/RHR)

Other support systems must also rigorously follow the same approach. For example the Electrical Power Supply (EPS) would have a claim numbers:

EPS SFC 2-1, with sub-numbers EPS 2-1.1, EPS 2-1.1 etc.

In this scheme every SFC is uniquely linked to the high level safety functions and each SFC, whether it is a frontline safety system or one of its support systems, has a unique number that can be readily tracked and cross checked across safety systems, their support systems and the requirements originating from the fault studies to ensure completeness.

As stated above, SPCs are claims which justify that the UK ABWR meets ther required system properties. A part of this process of developing SPCs is demonstrating relevant coverage of Hitachi-GE's NSEDPs. While SFCs describe the functions required of an SSC in order to achieve the requirements of the safety case, SPCs are system level properties such as redundancy, diversity and environmental qualification, which can help to fulfil many different safety functions. For this reason, SPCs are not directly linked to HLSFs, and the HLSF number is not used as part of the unique SPC

number. As mentioned in the preceding section, SPCs are unique within topic areas. The SPC number has the following structure:

(Topic Area identifier) SPC (SPC number)

e.g. Mechanical Engineering (**ME SPC 1**), Control and Instrumentation (**C&I SPC 1**), Electrical Power Supply System (**EPS SPC 1**).

Each engineering topic can derive its own set of Level 1 SPCs, but should;

- Develop a mapping between these and the relevant NSEDP principles.
- Ensure that all relevant NSEDP principles are covered by SPCs, and
- Ensure that each SPC 'Claim' is linked to the relevant System/sub system using a tabular format.

Depending on the granularity required to link claims to the relevant SSCs, the corresponding topic areas can develop claims further into sub-claims and arguments. These arguments can be managed by decomposing the SPC numbering '1' (for example to **ME SPC 1.1**) or by linking SPCs to specific systems (for example using the format **SSLC SPC 1**). When using the latter, the link between the claim and the argument is clearly defined. These detailed numbering formats are managed in each topic area. SPCs can be derived using a 'guide word' approach, where a series of guide words are chosen to represent groups of NSEDPs covering similar topics, such as 'fault tolerance', 'independence' and 'defence in depth'. Table 3 provides a generic list of guide words and links these to the relevant NSEDPs.

A three stage approach is taken to the production of SPCs using the guide word approach'.

Step 1: Consider the generic list of guide words and associated NSEDPs listed in Table 5.3-1 and confirm whether they are applicable to the topic/ discipline.

Step 2: Consider whether any additional guidewords are applicable to the topic/discipline, or are required to ensure coverage of all NSEDPs.

Step 3: For each applicable guide word produce a set of SPCs relevant to the discipline. A typical set of Level 1 SPCs based on the guide word approach are as follows where the 'ABC' represents the code for the SSC (e.g., RCIC, SSLC, etc.). Not all will apply to every SSC and some SSCs will have additional SPCs. In addition, the relevant NSEDPs shown in the table below are typical and each topic area with define the specific relevant NSEDPs in the process of defining SPCs.

Level 2 SPCs should be added where appropriate to ensure a readily understandable and traceable link to arguments and evidence. Completeness of the SPCs is important to safety as is the fact that they must demonstrate full coverage of the relevant NSEDPs. An example of the SPCs for a generic system (ABC) is shown in the table below together with the coverage of the NSEDPs. As the claims are developed into sub-claims and arguments the mapping to the NSEDPs should be retained but with enhanced detail in the claims tables provided in the supporting references to the relevant Generic PCSR Chapters.

Table 5.3-1 Generic Table of SPCs

SPC	Guide Word	Claim	Relevant NSEDPs
ABC SPC 1	Defence in Depth	System *ABC* has sufficient defence in depth to meet all relevant accident conditions, including suitable independence and diversity and suitable resilience to DBA, BDBA and SA events.	BP4.2, BP4.5, SP4.10.2 SP8.11.2, FP12 SP12.2.4
ABC SPC 2	Category and Class	The safety functions allocated to system *ABC* have been categorised and the SSCs classified in accordance with Hitachi-GE's SCDM.	BP4.6, SP4.6.1, SP4.6.2
ABC SPC 3	Reliability	The architecture of system ABC achieves the required reliability.	BP 4.10
ABC SPC 4	Fault Tolerance	System *ABC* is designed, selected and implemented to be tolerant of faults and tolerant of or resilient against failures caused by all relevant internal and external hazards (detailed in the fault schedule).	BP4.1, BP4.9, SP4.9.1 SP4.10.1, SP12.2.4
ABC SPC 5	Relevant Good Practice	System *ABC* is designed and implemented using relevant good technical practice and relevant good process practice, and will include codes and standards compliance.	BP4.1, SP4.10.3, SP4.12.5, FP8, BP8.1 BP8.2, BP8.3, BP8.4 BP8.7, FP9, FP11 BP11.1, BP11.3, BP15.1 SP15.1.2
ABC SPC 6	Lifecycle	The *ABC* design and selection considers all stages of the plant and hazard life cycles, including operation (including examination, maintenance, inspection and testing), in-life replacement and decommissioning. This also includes confirmation that components have been suitably qualified in accordance with Hitachi-GE qualification process.	SP4.5.1, SP4.6.3, SP4.10.4, SP5.2.5, BP8.1, BP8.2, BP8.5, BP8.6, BP8.8, BP8.9, BP8.10, SP8.10.1, BP11.3, SP13.2.3, SP15.1.1

ABC SPC 7	Human factors	Dependence on human actions for nuclear safety has been minimised to ALARP and human actions and human factors good practice have been taken into account in the design, the human interfaces and the operating procedures.	BP4.12, SP4.12.3, SP4.12.6, BP5.4, FP15
ABC SPC 8	Layout and Accessibility	System *ABC* equipment, components layout and accessibility is suitable in respect of safety requirements and hazard considerations, including safety requirements and emergency response considerations, and reduces risk to ALARP.	BP4.7, FP7, BP7.1, BP7.2, BP7.3, SP12.2.2
ABC SPC 9	Radiation Protection	System *ABC* meets the required Radiation Protection properties, including meeting all shielding, location and EMIT-derived requirements.	FP13, BP13.1, BP13.2, SP13.2.1, SP13.2.2, SP13.2.3, BP13.5, SP13.5.1, SP13.5.2, SP13.5.3, BP14.1, SP14.1.1, SP14.1.2, SP14.1.3, BP14.2, SP14.2.1, BP14.3, SP14.3.1, SP14.3.2, SP14.3.3, SP14.3.4

The terminology FP, BP and SP refer to Fundamental Principles, Basic Principles and Supporting Principles respectively specified in Hitachi-GE's NSEDP's [Ref 5.1-1]. The above table outlines the main principles of the SPC scheme. It is important to note that SPCs do not require to be rigorously aligned in their numbering system as is the case for the SFCs. This reflects the fact that each SSC will have varying properties and therefore the above list is representative. The key point is to use the topic area code and the numbering scheme to produce a unique claims number for each SPC within its relevant topic area. Once again, as with the SFCs, the SPCs can be broken down further into claims and arguments. Most engineering systems can use top level claims similar or identical to those given in table 3 above.

The demonstration of the full coverage of all the NSEDPs is presented in Topic Report on Compliance of UK ABWR Design with Nuclear Safety and Environmental Principles (NSEDPS) [Ref-5.6-5].

5.3.5 Safety Functions and definition of Human Based Safety Claims

Human actions are required to meet some of the Safety Functional Claims (SFCs) and Safety Property Claims (SPCs) of the SSCs of each system. Thus these human actions or HBSCs inherently support the achievement of the SFCs/SPCs defined in the preceding sections.

Because of the important role of human factors in ensuring that the relevant safety functions are delivered, the UK ABWR uniquely identifies these actions with the use of Human Based Safety Claims (HBSCs). The SCDM [Ref-5.6-4] Section 3.6 sets a requirement for the identification of HBSCs. The details on this scheme are described in Generic PCSR Chapter 27: Human Factors and the Human-Based Safety Claims Report [Ref 5.3-1] section 3.

5.4 Definition of Operating Stages, Modes and Conditions

5.4.1 Introduction

In this section, the operating stages throughout the plant life cycle, and the operating conditions during plant operations of UK ABWR design are defined.

5.4.2 Operating Stages

The lifecycle of a facility is broken down into discrete stages. The fundamental safety objectives apply for all stages in the lifetime of UK ABWR. The operating stages include planning, siting, design, construction, commissioning and commercial operation as well as decommissioning. The associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste are activities included within them.

5.4.3 Operating Modes and Plant Operating States

Commercial operation of the UK ABWR includes five Operating Modes which define the state of the power generation facilities. These operating modes for BWRs have long been established and the UK ABWR follows the same practice – five modes are identified:

(1) Power operation
(2) Start-up
(3) Hot shutdown
(4) Cold shutdown, and
(5) Refuelling outage

Each of these operating modes has clearly defined entry and exit conditions. Movement from one mode to another is carefully managed as it is recognised changing plant state is a planned activity.

(1) Power operation
In this mode, the reactor is critical and the turbines are put into operation to generate power. This mode starts when the mode switch is changed to ‘run’ position.

(2) Start-up
At the beginning of this mode, the reactor is in a shutdown mode with all control rods inserted. This mode starts when the mode switch is changed to ‘start-up’ position. During this mode the control rods are withdrawn from the core and the reactor is taken critical. When the mode switch is selected ‘run’, this mode moves on to Power Operation mode.
During this mode, the reactor could be brought to a temporary “Hot standby” state if necessary (for example, when the plant is disconnected from the electrical network). During this state the reactor is kept critical ready to resume operation.

(3) Hot shutdown
In this mode, the reactor is sub-critical. This mode starts when the mode switch is changed to ‘shutdown’ in the shutdown process. During this mode the control rods are inserted and the reactor is taken sub-critical. This mode moves on to Cold shutdown when coolant temperature is lower than or equal to 100°C.

(4) Cold shutdown
The shutdown process takes the plant from hot shutdown to the cold shutdown when reactor coolant temperature is lower than or equal to 100°C with the reactor sub-critical.

(5) Refuelling outage
Once the plant is in a cold shutdown, refuelling outage operations may begin. This involves the flooding of the reactor well, removal of the vessel head and upper internals (steam separator and dryer) and removal of fuel to the spent fuel pool. New fuel is introduced and the plant made ready for start-up. During the refuelling outage, many essential maintenance tasks are carried out.

For fault studies and PSA, the definition of Operating Modes given here is not fine enough to allow for differences in configuration of reactor and Spent Fuel Storage Pool (SFP) required to properly asses faults. Therefore, Generic PCSR Chapters 24: Design Basis Analysis to Chapter 26: Beyond Design Basis and Severe Accident Analysis use the following Plant Operating States (POS) (Chapter 24: Design Basis Analysis uses the C-1 to C-6 notation and Chapters 25: Probabilistic Safety Assessment and 26: Beyond Design Basis and Severe Accident Analysis uses POS X). The relationship between the POS and the operating modes (1) to (5) previously defined is shown below. Refer to Generic PCSR Chapter 24 section 24.10.2 'Reactor Faults in Shutdown Modes' for further details.

State A – Normal At-Power Operations (POS F)
This plant operating state corresponds to operating modes (1) and (2).

C-1 – Transition to Reactor Cold Shutdown (POS S)
RPV assembled and isolated, SFP isolated, RPV head and PCV head on, SFP gate closed
This plant operating state corresponds to operating mode (4).

C-2 – Transition to Reactor Disassembled and Reactor Well Gate Open (POS A)
RPV disassembled but isolated, SFP isolated, RPV head off, SFP gate closed
This plant operating state corresponds to operating mode (5).

C-3 – Full Water Level in Reactor Well and Gate Open (POS B-1, B-2)
RPV Disassembled, Pools System Combined, SFP gate open
This plant operating state corresponds to operating mode (5).

C-4 – Transition to Closed Condition of PCV/RPV Top Heads (POS C)
RPV disassembled but isolated, SFP isolated, PCV head off, RPV head on, SFP gate close
This plant operating state corresponds to operating mode (5).

C-5 – Preparation of plant startup (POS D)
RPV assembled and isolated, SFP isolated, RPV head and PCV head on, SFP gate closed
This plant operating state corresponds to operating mode (4).

C-6 – Full core off-loaded to the SFP (POS E)
No fuel in RPV, SFP isolated, SFP gate closed
This plant operating state corresponds to operating mode (5).

5.4.4 Operating Conditions

Operating Conditions are defined below and are used for evaluation in Mechanical Engineering (ME) and Structural Integrity (SI) fields. The Operating Condition definitions include the terms 'fault' and 'event' which are separately defined in Section 5.5 of this chapter.

5.4.4.1 Operating Conditions

The operating conditions are defined in the following sub-sections 5.4.4.2 (1) to (4) according to the events during operation of the Nuclear Power Plant (NPP).

(1) Operating Condition I
(2) Operating Condition II
(3) Operating Condition III, and
(4) Operating Condition IV

5.4.4.2 Definition of Operating Conditions

(1) Operating Condition I:
Operating Condition I is the condition during commercial operation where the Expected Events defined in Section 5.5 can take place during all the operational modes. Operating Condition I includes all conditions different from upset, emergency, faulted, or testing conditions. In other words, Operating Condition I is the premeditated operations or the transition period between the operation modes.

(2) Operating Condition II:
Operating Condition II is a condition with Foreseeable Events or a part of Frequent Faults defined in Section 5.5 deviating from Operating Condition I and other than Operating Condition III, IV and Test Condition. The deviation is caused by any single failure of equipment, any single operator error or control malfunction, a loss of load or power, etc. anticipated in service period of NPP.

(3) Operating Condition III:
Operating Condition III is a condition with the rest of Frequent Faults or a part of Infrequent Faults defined in Section 5.5 deviating from Operating Condition I, which requires shutdown. This condition is included to provide assurance that no gross loss of structural integrity will result as a concomitant effect of any damage developed in the system. The emergency conditions include infrequent operating transients caused by a multiple valve blowdown of the reactor vessel such as inadvertent actuation of Automatic Depressurisation System (ADS), reactor overpressure with delayed scram or Anticipated Transient Without Scram (ATWS), a small line break Loss of Coolant Accident (LOCA) including crack and etc., which have sufficient lower probability than Operating Condition II.

(4) Operating Condition IV:
Operating Condition IV is a condition with the rest of Infrequent Fault whose consequences are such that the integrity and operability of the system may be impaired to the extent that considerations to public health and safety are involved. Though these events are infrequent during service period of the NPP, they are postulated to demonstrate the validity of the design just in case of occurrence. This condition includes, but is not limited to, LOCAs, which are the most severe events that must be considered in the design and thus represent the limiting design base.

5.4.5 Safe Shutdown Condition

The safe shutdown condition applies to the reactor and is defined as the reactor state when reactor cold shutdown has been achieved.

The UK ABWR design is capable of achieving reactor cold shutdown within 36 hours after SCRAM even without cooling via the main condenser, such as would be the situation following a Loss of Offsite Power (LOOP), and also assuming any single failure within the claimed safety systems.

5.4.6 Test Condition

Test Condition is a term generally used in BWRs which refers to the conditions under the shop and field hydrostatic tests conducted to verify the integrity of the SSCs forming part of the Reactor Coolant Pressure Boundary (RCPB) in the ME and SI fields.

5.4.7 Terminology Used in Claims Tables

The following is used:

(1) Normal Conditions: refers to operating modes (1) to (5) defined in section 5.4.3 of this chapter. These are operations in the non-fault conditions.
(2) Fault Conditions: this represents the start of a sequence or a plant state following a fault occurring in an SSC or Safety Related Design Provision. Faults are described in section 5.5 of this chapter.
(3) Operating Conditions I to IV: this is the same as the Operating Conditions specified in section 5.4.4 of this chapter.
(4) Test Condition: this is the same as the Test Condition specified in section 5.4.6 of this chapter.

5.5 Definition of Design Basis Faults and Beyond Design Basis Faults

It is an important principle in the design of modern nuclear facilities that they should be "fault tolerant", which means that faults and other disturbances to normal operating conditions should not lead to undesirable consequences. The safety of plant is assured by several layers of protection. This protection is provided by Structures, Systems, and Components (SSCs) that deliver the safety functions necessary to protect the plant from undesirable consequences in normal operating conditions and following faults. This leads to the identification of a number of categories of events, defined by their frequencies and/or potential consequences.

Categorisation may be based on targets related to frequency, consequence or risk and are related to two levels, defined in the NSEDPs:

- Basic Safety Level (BSL) – this defines the boundary between acceptable and unacceptable consequences. Provision must be made in the design to prevent any potential consequences above the BSL.

- Basic Safety Objective (BSO) – this defines a target which is expected to be achieved by all new plant. Consequences below the BSO are deemed to be broadly acceptable.

Events are also divided into two broad groups by frequency. Frequent events have a frequency greater than once in 1000 years of operation; infrequent events less than or equal to once in 1000 years.

The categories of events and faults identified for UK ABWR are as follows:

- Expected Events
- Foreseeable Events
- Design Basis Faults
- Beyond Design Basis Faults, and
- Severe Accidents

(1) Expected Events

The events are expected to occur at least once during the lifetime of the plant. It is expected that their effect on the plant should be minimal, amounting to no more than a mild deviation from normal operating conditions and consequences below the BSO without any mitigating actions.

(2) Foreseeable Events

Foreseeable events are frequent events with unmitigated consequences below the BSL. However, it is possible that some mitigation action is required to reduce consequences below the BSO.

(3) Design Basis Faults

Design Basis (DB) Faults are faults whose potential unmitigated consequences would be above the BSL and whose initiating event frequency is greater than once in one-hundred thousand years (10^{-5} /y). Because such consequences are unacceptable, it is necessary for the design to make provision for these consequences to be prevented or reduced.

If a sequence, that is an initiating event plus the failure of the provided prevention or mitigation, has a frequency greater than once in ten million years (10^{-7} /y) then the sequence is also considered to be a Design Basis Fault.

DB Faults are divided into infrequent faults and frequent faults (See Table 5.5-1), which are DB faults with initiating event frequency greater than once in a thousand years (10^{-3} /y).

(4) Beyond Design Basis Faults

Beyond Design Basis (BDB) Faults are faults whose unmitigated consequences lie above the BSL but whose frequencies are below the cut-off for infrequent DB faults. Such faults may be treated as DB faults (i.e. subject to conservative DB analysis) but there is no formal requirement to do so. It is, however, required to demonstrate that there are no "cliff-edge" effects near the design basis boundary and that risks are ALARP.

(5) Severe Accidents

Severe accidents are defined as those fault sequences that could lead either to consequences exceeding the highest off-site radiological doses given in the BSL of NSEDP Target 4, or to an unintended relocation of a substantial quantity of radioactive material within the facility which places a significant demand on remaining physical barriers.

The definition of the categories of faults and events used for UK ABWR in this Generic PCSR are summarised in Table 5.5-1.

Table 5.5-1: Faults and Events Categories

Fault /Event Category		Fault Frequency (/y)	Potential Consequences	
			Off-site	On-site
Design Basis Faults	Frequent DB Faults	$F \geq 10^{-3}$	> 1 mSv (BSL)	> 20 mSv (BSL)
	Infrequent DB Faults	$10^{-4} \leq F < 10^{-3}$	> 10 mSv (BSL)	> 200 mSv (BSL)
		$10^{-5} \leq F < 10^{-4}$	> 100 mSv (BSL)	> 500 mSv (BSL)
Beyond Design Basis Faults		$10^{-7} \leq F < 10^{-5}$	> 100 mSv	> 500 mSv
Foreseeable Events		$F > 10^{-3}$	0.01 mSv (BSO) to 1 mSv (BSL)	0.1 mSv (BSO) to 20 mSv (BSL)
Expected Events		$F > 10^{-2}$	< 0.01 mSv (BSO)	< 0.1 mSv (BSO)

The values for the BSL and BSO in the above table are taken from the NSEDPs.

These categories are shown diagrammatically in Figure 5.5-1.

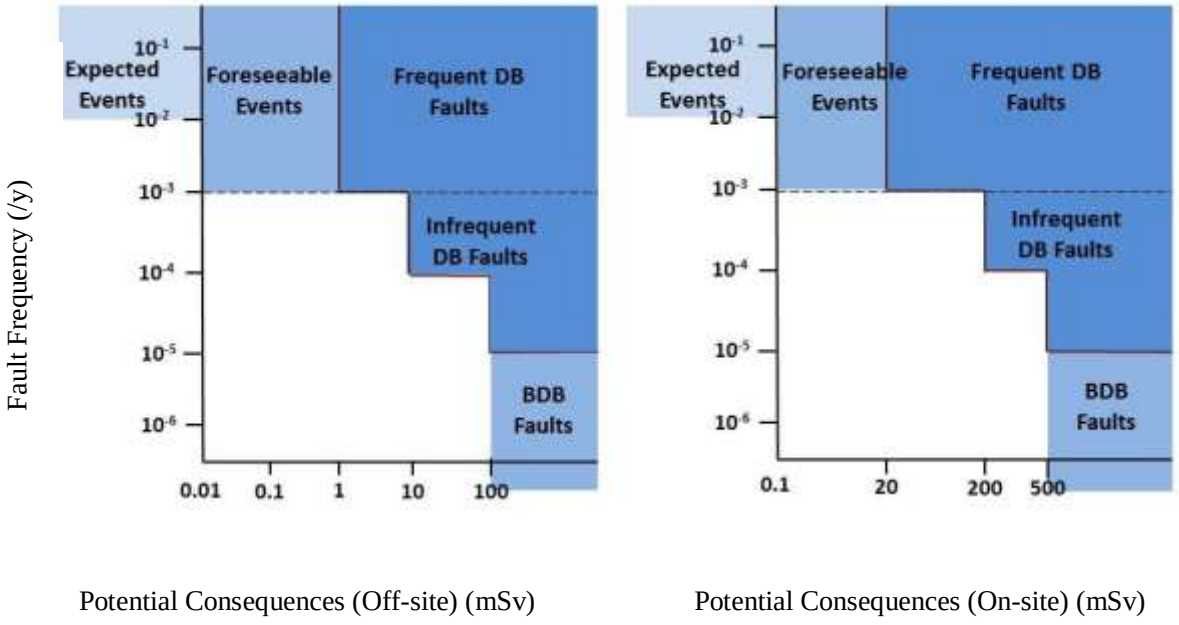


Figure 5.5-1: Faults and Events Categories

5.6 Categorisation of Safety Functions and Classification of Structures, Systems and Components (SSCs)

The categorisation of safety functions and the classification of the structures, systems and components (SSCs) that deliver them are important parts of the development of safety cases. This section covers the purpose and methodology for categorisation and classification used in the UK ABWR safety case.

5.6.1 Summary Description of Safety Categorisation and Classification

The safety of plant in the UK ABWR is assured by several layers of protection. This protection is provided by Structures, Systems, and Components (SSCs) that deliver the safety functions necessary to protect the plant from undesirable consequences in normal operating conditions and the following faults. These safety functions are identified by analysis of the causes and consequences of plant failures and are categorised according to their importance to the overall safety of the plant. The SSCs that deliver these safety functions are then classified according to their importance in delivering the corresponding safety functions. The classification reflects the importance of each SSC to the safety of the plant and links engineering, such as codes and standards for design, manufacture, inspection, maintenance, and testing directly to the safety case.

The safety categorisation and classification processes are important steps in the overall design assessment process, whose main purpose is to ensure that the plant is designed, manufactured, installed, commissioned, operated, and maintained in a manner that is commensurate with each SSC's importance to safety.

The process of categorisation starts with the systematic and comprehensive identification of faults and their categorisation according to their potential unmitigated consequences and frequency as described in Section 5.5. Safety functions are identified to prevent or reduce the radiological risk for all identified faults and they are then categorised according to their importance for safety.

Safety functions that prevent faults and those that mitigate consequences are related to the three fundamental safety functions identified by IAEA:

(i) Control of reactivity,
(ii) Removal of heat from the reactor and from the fuel store, and
(iii) Confinement of radioactive material.

This last fundamental safety function is taken to include shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Design provision is then made for each safety function and the resultant safety measures are classified according to their importance in delivering the associated safety function(s).

The classification is then used to ensure that SSCs are designed and operated using codes, standards and procedures commensurate with their importance for safety as expressed in their safety classification and the categorisation of the safety function(s) they deliver. Finally, deterministic and probabilistic safety assessments demonstrate that the resulting design meets all risk targets and reduces risks so far as is reasonably practicable.

The following sections describe the categorisation and classification scheme used in the UK ABWR safety documentation and is based on guidance given in the Nuclear Safety and Environmental Design Principles (NSEDPs) which are largely based on the ONR Safety Assessment Principles, by the International Electrotechnical Commission [Ref-5.6-1] and in IAEA Standards [Ref-5.6-2].

5.6.2 UK ABWR Safety Functions

The Safety Functions for the UK ABWR have been developed systematically from two major safety category groups. Following the IAEA approach [Ref-5.6-3], one group is referred to as design provisions and includes the group of safety functions whose failure could cause abnormal conditions at nuclear power plant facilities, thereby leading to undue radiation exposure to the public or site personnel. Also included in this group are SSCs required for normal operation, for example the reactor pressure vessel, the gross failure of which would lead directly to unacceptable consequences. In line with IAEA guidance [Ref-5.6-3] such SSCs can be classified directly.
The other group contains those whose function is to prevent an escalation of such condition or put such conditions under immediate control in case of abnormal conditions at nuclear power plant facilities thereby mitigating possible radiation exposure to the public or site personnel.

For the UK ABWR the five identified fundamental safety functions defined below are closely linked to one of the three fundamental safety functions described in the IAEA documents [Ref-5.6-2] [Ref-5.6-3]:

(1) Control of reactivity
(2) Fuel cooling
(3) Long term heat removal
(4) Confinement/Containment of radioactive materials, and

(5) Others (largely for support functions required to enable one or more of the above safety functions)

A full list of UK ABWR high level safety functions (HLSFs) identified from above development is shown in Table 5.6-1. These safety functions have been and will continue to be confirmed and, if required, updated and extended during the fault studies performed by the future licensee.

Table 5.6-1 : High level safety functions in UK ABWR (1/2)

Fundamental Safety Function	No.	High Level Safety Functions
1. Control of Reactivity	1-1	Functions to prevent excessive reactivity insertion
	1-2	Functions to maintain core geometry
	1-3	Emergency shutdown of the reactor
	1-4	Functions to maintain sub-criticality
	1-5	Function of alternative reactivity control
	1-6	Functions to circulate reactor coolant (functions to control reactivity of the core in normal operational states)
	1-7	Functions to plant instrument and control (except for safety protection function) (Functions to control reactivity of the core in normal operational states)
	1-8	Functions to suppress reactor power increase with other system
	1-9	Functions to maintain sub-criticality of spent fuel outside the reactor coolant system
	1-10	Functions to maintain sub-criticality of spent fuel during processes of spent fuel removal from cask pit to storage area and during interim storage period
2. Fuel Cooling	2-1	Functions to cool reactor core
	2-2	Function of alternative fuel cooling
	2-3	Function to make up reactor coolant with other system
	2-4	Function to cool spent fuel outside the reactor coolant system
	2-5	Functions to make up water for spent fuel pool
	2-6	Functions to maintain spent fuel temperature during processes of spent fuel removal from cask pit to storage area and during interim storage period
3. Long term heat removal	3-1	Functions to remove residual heat after shutdown
	3-2	Function of alternative containment cooling and decay heat removal
4. Confinement /Containment of radioactive materials	4-1	Functions to form reactor coolant pressure boundary
	4-2	Functions to prevent overpressure within the reactor coolant pressure boundary
	4-3	Functions to contain reactor coolant outside the RCPB
	4-4	Functions to contain radioactive material
	4-5	Functions to reseat safety valves and relief valves
	4-6	Functions to mitigate reactor pressure increase with other system (other than No.4-2)
	4-7	Functions to confine radioactive materials, shield radiation, and reduce radioactive release
	4-8	Functions to minimise the release of radioactive gases
	4-9	Functions to contain radioactive materials in the event of a severe accident
	4-10	Functions to prevent the dispersion of fission products into reactor coolant, spent fuel pool and canister
	4-11	Functions to store the radioactive materials as gaseous waste
	4-12	Functions to store the radioactive materials as liquid wastes
	4-13	Functions to store the radioactive materials as solid wastes
	4-14	Functions to provide containment barrier during processes of spent fuel removal from cask pit to storage area and during interim storage period
	4-15	Unused number
	4-16	Functions to provide radiation shield during processes of spent fuel removal from cask pit to storage area and during interim storage period
	4-17	Functions to maintain PCV atmosphere in an inert state for preventing hydrogen combustion

Table 5.6-1: High level safety functions in UK ABWR (2/2)

Fundamental Safety Function	No.	High Level Safety Functions
5. Others	5-1	Functions to generate actuation signals for the engineered safety features and reactor shutdown systems
	5-2	Supporting functions especially important to safety
	5-3	Function of alternative supporting system
	5-4	Monitoring functions of plant conditions to support operator actions
	5-5	Functions to shut down safely from outside the control room
	5-6	Functions to handle fuel and heavy equipment safely
	5-7	Functions to limit the effect of hazard
	5-8	Functions to clean up reactor coolant
	5-9	Functions to clean up water except for reactor coolant
	5-10	Functions to supply electric power (except for emergency supply)
	5-11	Supporting functions to supply power (except for emergency supply)
	5-12	Supporting functions for management of normal operation
	5-13	Auxiliary functions for plant operation
	5-14	Supporting functions for on-site emergency preparedness
	5-15	Functions to control hydrogen concentration in fault conditions
	5-16	Functions to provide handling and retrievability during processes of spent fuel removal from cask pit to storage area and during interim storage period
	5-17	Function to provide structural support to SSCs
	5-18	Function to maintain internal building environment appropriate for SSC
	5-19	Monitoring functions of radioactive discharge to the environment
	5-20	Functions to maintain availability of CRs hydraulic insertion function and to recover CRs to normal unlatched state after rapid insertion
	5-21	Function to retain water for provision of radiation shield during the refuelling process
	5-22	Function to limit deceleration loading to canister containment boundary during credible cask drop faults
	5-23	Monitoring functions of occupational and public radiation exposures
	5-24	Functions to limit worker access into high dose area

5.6.3 Categorisation of Safety Functions

For each event identified in the UK ABWR Fault Schedules, it is necessary to identify what needs to be done to reduce the risk to acceptable levels, that is, to identify the safety functions that must be provided in each case to reduce risks, so far as is reasonably practicable, below the BSO level.

In the hierarchy of protective measures, prevention is more desirable than mitigation. However, in practice, which approach is followed for a particular fault needs to take account of whether potential safety measures are reasonably practicable to implement. For some faults (for example, RPV failure), no mitigation is reasonably practicable and prevention is the only option available. For others, only mitigation is reasonably practicable, either because prevention would require a level of engineering beyond what is reasonably available (for example, faults in the turbine and steam system) or because the cause of the event is outside the control of plant operators (for example, loss of off-site power).

Following the NSEDPs, three categories of safety functions are identified:

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, and

Category C - any other safety function

The approach to categorisation of safety functions is based on the radiological consequences (risks) of faults and events.

Consequences that are greater than the BSL of Target 4 and with initiating fault frequency $\geq 10^{-5}$ /y, that is, those within the Design Basis (DB) region, are deemed to be intolerable and must be removed by design, either by identifying safety functions that prevent the failure that leads to the risk or by identifying safety functions to reduce the risk to acceptable levels.

Safety functions identified in this way from the Design Basis assessment are deemed to play a principle role in ensuring nuclear safety and are thus categorised as Category A:

Category A Category A safety functions play a principle role in ensuring nuclear safety in that they are associated with the removal of intolerable radiological risks from DB faults by either prevention of the risks or reduction of the risks to broadly acceptable levels.

The total set of such safety functions constitutes the design basis for the plant – the design must provide suitable means to deliver them all.

Consequences that are less than the BSL but greater than the BSO (Foreseeable Events) or > BSL with initiating fault frequency < 10^{-5} /y (Beyond Design Basis faults) are deemed to be tolerable, provided consequences are kept as low as reasonably practicable. The approach to these risks is similar to that for intolerable risks except that the risks may be deemed acceptable if it can be shown that there are no additional reasonably practicable means of (further) preventing or of reducing them. Safety functions defined in this way from assessments of Beyond Design Basis faults or Foreseeable Events are deemed to make a significant contribution to nuclear safety and are thus categorised as Category B. Functions whose failure would lead to a demand on a Category A safety function are also deemed to make a significant contribution to nuclear safety and categorised as B:

Category B Category B safety functions make a significant contribution to nuclear safety in that they are associated with the removal of radiological risks outside the design basis by either preventing the risks or reducing the risks to broadly acceptable levels for Foreseeable events and Beyond-Design-Basis (BDB) faults, which are identified in fault studies.

Functions whose failure would lead to a demand on a Category A safety function are also categorised as B.

Where an assessed risk is in the Foreseeable event or BDB fault region but is close to the boundary, then serious consideration should be given to assign the event to the DB region, particularly if there are large uncertainties in the consequences or frequency. The corresponding safety functions should then be categorised as Category A.

Consequences of failures that are less than the BSO are deemed to be broadly acceptable and no action is required in the design to prevent or reduce them and they are considered to be part of normal operation. However, such risks are still subject to ALARP consideration and safety functions may be identified in the ALARP process. In the special case of Expected Events relating to environmental protection, there is a requirement to show that BAT has been applied.

Safety functions not categorised as Category A or Category B, particularly any defined in ALARP or BAT assessments are categorised as Category C.

Category C Category C safety functions are those that do not fall into either of Categories A or B. They are mainly associated with the support of Category A or B safety functions or identified from ALARP or BAT analyses.

Any function which does not meet any criteria of the three basic categories above is screened out of categorisation process and is designated as non-categorised.

Categorisation of most of safety functions relies on the fault studies presented in Chapter 24: Design Basis Analysis and Chapter 26: Beyond Design Basis and Severe Accident Analysis of this Generic PCSR.

5.6.4 Structures, Systems and Components Important for Safety and their Classification

The Safety Measures or Structures, Systems and Components (SSCs) which deliver the Safety Functions identified earlier are classified according to their importance in delivering the corresponding safety function. This classification is the basis on which codes and standards, materials, manufacturing quality criteria, and procedures for examination, maintenance and testing are selected for each SSC in the plant. Please note that human based safety claims are a very important part of the overall concept of a safety measure and all such claims follow the principles specified in this document. More information is given in Chapter 27: Human Factors of this Generic PCSR and throughout this Generic PCSR where human based safety claims are made.

As with safety functional categorisation, following the NSEDPs, three classes of SSCs are identified:

Class 1 - any structure, system, or component that forms a principal means of fulfilling a Category A safety function

Class 2 - any structure, system, or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function, and

Class 3 - any other structure, system, or components

From these definitions, it follows that any SSC claimed in the safety case as the first-line means of delivering a Category A safety function must be Class 1.
From this basic understanding, it also follows that SSCs claimed as secondary or diverse means of delivering a Category A safety function must be at least Class 2, as must the first-line means claimed as delivering Category B safety functions.

Thus, the basic scheme for classifying SSCs is:

Class 1 SSCs claimed as being the principle or first-line means of delivering Category A safety functions and referred to as A1.

Class 2 SSCs claimed as being the second line or diverse means of delivering a Category A safety function, or the principle or first-line means of delivering a Category B safety function, and referred to as A2 and B2 respectively.

Class 3 SSCs claimed as providing a third-line means of delivering a Category A safety function, a second-line means of delivering a Category B safety function or as delivering a Category C safety functions, and referred to as A3, B3 and C3 respectively.

For all reactor faults the followings are the simple deterministic rules for the safety classification applied for the UK ABWR. A1 SSCs are those claimed in the safety case as being the first-line means of protection against Design Basis faults. For frequent Design Basis faults (that is, Design Basis faults with frequency greater than 10^{-3}/y), each identified safety function is required to have a diverse means of delivery. SSCs claimed to provide this diversity are classified as at least A2.
For both reactor and non-reactor faults B2 SSCs are identified to provide Category B safety functions in Beyond Design Basis assessments or in the protection against Foreseeable Events.

A3, B3 and C3 SSCs have safety importance but do not fulfill the requirements specified for A1, A2 and B2 SSCs. The analysis of Expected Events (which are part of normal operations) may identify functions that need to be fulfilled to satisfy BAT requirements. Such functions are categorised as category C and any SSCs identified to fulfill them are classified as Class 3 and referred to as C3.

In the design, there are a number of SSCs whose failure or maloperation would lead to a demand on a Category A safety function. These SSCs are deemed to provide Category B safety functions and are, therefore, classified as B2 or B3, or directly classified as Class 2 or Class 3. For the UK ABWR, such SSCs are classified:

- B2 or Class 2 if there is an A1 means of protection against their failure or maloperation leading to a design basis fault.
- B3 or Class 3 if there are two diverse means of protection against their failure or maloperation leading to a design basis fault by A1 and A2 SSCs (A1 + A2). This represents a proportionate approach to safety classification but is subject to the usual process of ensuring that risks are as low as reasonably practicable.

The SSCs that can be directlty safety classified are those whose primary role is to support normal operation. Auxiliary services that support components of a system important safety are considered part of that system and are classified accordingly, unless failure does not prejudice successful delivery of the safety function. These are treated as follows:

- Essential support and service systems; Supporting systems directly needed for a system important to safety to fulfill its safety functions are considered to have the same class as the supported system.

- Non essential support and service systems; Supporting systems needed for a system important to safety to maintain or assure its reliability but not directly needed to fulfill its safety functions are considered to have an importance that may be lower than that of supported system. However, such systems must be at least Class 3.

Appropriately designed interfaces are provided between SSCs of different classes to ensure that any failure in a lower class SSC do not propagate to a SSC of a higher class. Equipment providing the function to prevent the propagation of failures are assigned to the higher class of the interfacing SSCs. When SSCs of different classes are connected, design requirements equivalent to those for higher class shall be applied to the lower class. Alternatively, adequate functional isolation by means of, for example, isolation devices designed to the higher class shall be implemented so that safety functions of SSCs of higher class are not impaired of the failure of lower class SSCs.
SSCs with two or more safety functions shall meet every design requirement for the safety functions to be fulfilled.

The above classification scheme is based on a fully deterministic approach. In the development of this Generic PCSR, Probabilistic Safety Assessment (PSA) is used to assess the importance of SSCs through the assignment of importance measures such as Risk Achievement Worth (RAW). This process may lead to the classification of some SSCs being revised.

5.6.5 Provision of Safety Functions

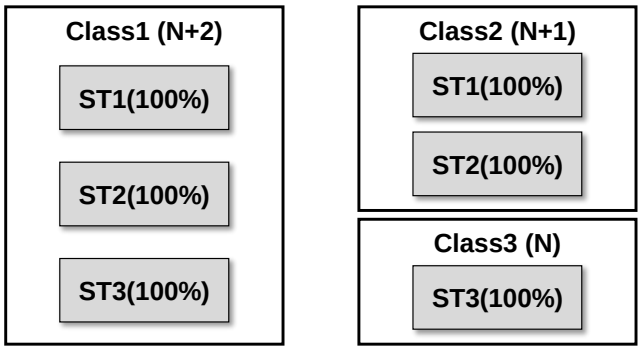
As described earlier for Design Basis reactor faults, it is conservatively assumed that the unmitigated consequences are greater than 100 mSv off-site and/or 500 mSv on-site. For all reactor frequent Design Basis faults Category A Safety Functions are provided by a Class 1 system, backed up by a diverse system of at least Class 2. The rationale for this is based on the normal range of probability of failure on demand that can be claimed for various classes of systems, as shown in the table below:

Table 5.6-2: Safety Class and Probability of failure-on-demand (pfd) ranges

System Class	Redundancy	pfd
Class 1	N+2 (single failure criterion)	$10^{-4} \leq pfd < 10^{-3}$
Class 1 including diversity	N+2 (single failure criterion)	$10^{-5} \leq pfd < 10^{-4}$
Class 2	N+1	$10^{-3} \leq pfd < 10^{-2}$
Combination of Class 1 and Class 2	(N+2) +(N+1)	$10^{-8} \leq pfd < 10^{-5}$
Class 3	N	$\geq 10^{-2}$

For infrequent faults ($10^{-3} > f \geq 10^{-5}$/y) with class 1 provision and for frequent faults ($f \geq 10^{-3}$/y) with Class 1 and diverse Class 2 provision, the sequence frequency is evaluated to be $< 10^{-7}$/y. This ensures that the Design Basis criteria are met, that is, that the mitigated risk is less than BSO and the sequence frequency is less than 10^{-7}/y.

It is normally assumed that the Class 1 SSC providing the Category A Safety Function is a single system with N+2 redundancy, especially for active systems containing active components whose functioning depends on an external input such as actuation, mechanical movement or supply of power. However, this is not necessarily the case for other facilities. It is possible to construct an equivalent Class 1 system by combining lower class systems as Class 2 and Class 3 as illustrated in Figure 5.6-1 below.



Note: ST is 'safety train' which means the totality of electrical, mechanical, human and other features required to deliver a safety function.

Figure 5.6-1: Equivalency of an A1 SSC with combination of lower class systems

This equivalency applies only if the following criteria are met:

- The single failure criterion must be met by the combined systems;
- There must be a comprehensive safety justification for the independence between the two lower class systems based on the application of robust dependent failure analysis against the cause of Common Cause Failure (CCF);
- All the systems must be environmentally qualified for the conditions where the category A function is required; and.
- All sequences involving the combined system must meet probabilistic targets, taking account the dependent failure analysis outcomes specified above.

For Design Basis faults in other areas of the plant (that is, not involving the reactor) the consequences may be less than for reactor faults as the overall unmitigated risk is also less. Additionally the time it takes to respond to non-reactor faults is often much longer and this can be used [Ref-5.6-3] as a justification for adjusting strictly deterministic rules. In order to meet overall risk targets it may therefore not be necessary that all Category A Safety Functions are provided by class 1 SSCs. Using a similar argument to that above giving the rationale for reactor faults, different provision of Category A Safety Functions can be justified. In particular, for some lower consequence faults, it may be justifiable to provide the Category A Safety Function with a Class 2 SSC.

More information is provided on applying deterministic rules guided by probabilistic insights in the Safety Case Development Manual for the UK ABWR [Ref-5.6-4].

5.6.6 Application of Safety Classes

The categorisation and classification scheme developed in this section reflects a comprehensive view as to how individual safety functions and the SSCs that deliver them play their role in the overall safety of the plant. However, there are different considerations with respect to specific aspects of SSCs and for specific types of events, which are discussed in this sub-section.

(1) Codes and Standards

Appropriate nuclear codes and standards are adopted for SSCs in Classes 1 and 2. If there are no appropriate nuclear codes and standards, an approach derived from equivalent non-nuclear codes and standards is applied. For SSCs in Class 3, appropriate non-nuclear-specific codes and standards are applied. The exception to this is control and instrumentation (C&I) which does have nuclear specific codes. Details of codes and standards adopted for UK ABWR are given in the Codes and Standards section of this chapter of the Generic PCSR.

(2) Examination, Maintenance, Inspection and Testing (EMIT) Requirements

In principle, all Class 1, Class 2 and Class 3 structures require Examination, Maintenance, Inspection and Testing (EMIT). However, the specific requirements for EMIT (frequency, type, etc.) are assigned according to the reliability claimed for each safety measure and the SSC's classification.

(3) Seismic Design

Each SSC is assigned to a seismic category that corresponds to the consequences of failure, either in terms of any requirement on the SSC to provide its safety function during and following a seismic event or in terms of radiological dose (on-site / off-site consequences) in case of the SSC failing due to the seismic event.

(a) Seismic Category 1

Seismic Category 1 SSCs are designed to withstand the Design Basis Earthquake (DBE - probability of exceedance per annum of 10^{-4} estimated on a conservative basis) and are required to maintain structural and functional integrity in combination with other appropriate loads. These SSCs are those necessary to ensure the capability to prevent or mitigate the consequences of seismic events which could result in a potential on-site unmitigated dose consequence >200mSv or off-site unmitigated dose consequence >10mSv evaluated on a conservative basis. Additionally, the requirement is applied to SSCs which are required in the event of a Beyond Design Basis accident which contains a seismic event as a part of the fault sequence.

(b) Seismic Category 1A

Seismic Category 1A SSCs are designed to withstand the DBE (probability of exceedance per annum of 10^{-4} estimated on a conservative basis) in combination with other appropriate loads without spatial interactions or any other interactions with Seismic Category 1 SSCs.

(c) Seismic Category 2

Seismic Category 2 SSCs are designed to withstand less than the DBE (probability of exceedance per annum of 10^{-3} estimated on a conservative basis) and are required to maintain structural and functional integrity in combination with other appropriate loads. These SSCs are those necessary to ensure the capability to prevent or mitigate the consequences of seismic events which could result in a potential on-site unmitigated dose consequence >20mSv or off-site unmitigated dose consequence >1mSv evaluated on a conservative basis.

(d) Seismic Category 3

Nuclear safety related SSCs that are not categorized as Seismic Category 1, 1A or 2 are designated as Seismic Category 3. There should not be a disproportionate increase in risk due to low consequence frequent hazards just outside the design basis; these risks are therefore be demonstrated to withstand the Operating Basis Earthquake (OBE) as defined by the site and be ALARP. For some facilities, the external hazard loads may be bounded by the application of normal industrial UK standards.

(e) Beyond Design Basis Earthquake

Adequate seismic margins for the loss of safety functions must be demonstrated for the Beyond Design Basis Earthquake. To ensure that the performance of SSCs against the relevant Safety Functions is adequate, either a seismic margin assessment or PSA analysis is performed to ensure no cliff-edge effects.

(4) Structural Design

There are some components, usually providing the confinement safety function, that are special cases of Class 1 because there is no reasonably practicable means of adequately mitigating their failure. As stated earlier these design provisions are directly classified.

These special cases are invoked where:

(a) A metal component or structure forms a principal means of ensuring nuclear safety;

(b) The estimated likelihood of gross failure needs to be very low or the safety case claims that gross failures can be discounted.

Components where the safety case claims that gross failure can be discounted are classified as "Very High Integrity" and are generally those Class 1 components forming part of the pressure boundary with no reasonably practicable means of protecting against their failure.

An example of the 'Very High Integrity' component is the UK ABWR Reactor Pressure Vessel (RPV). The RPV's Major Boundary Portion like the Shell, Top Head, Bottom Head, Nozzles etc. are required to have a very low frequency of gross failure. However such low frequencies cannot be demonstrated using actuarial statistics because of a lack of data, and cannot be plausibly or confidently estimated using theoretical modeling. Instead the approach is to develop a so-called incredibility of failure safety case that gives a high level of confidence in the reliability of the vessel to deliver its required safety function throughout its life.

If there is a single line of protection with no redundancy against the failure of such Class 1 components, they are classified as "High Integrity". The safety case for these components does not require the same level of robustness as a VHI Safety Case although because they are Class 1 their safety case still requires in-depth and comprehensive consideration of all relevant factors.

If there is a single line of protection with redundancy against the failure of such Class 1 components, they are designated as "Standard Class 1" and treated as any other Class 1 SSC.
The development and application of this classification for the structural integrity of Class 1 SSCs is given in Generic PCSR Chapter 8: Structural Integrity.

5.7 Qualification of SSCs

5.7.1 Introduction

This section defines the service conditions with respect to the Plant Operating Conditions for the mechanical and electrical equipment and the related structures delivering the safety function. It also documents the qualification methods and procedures employed to demonstrate the capability of this equipment to perform safety functions when exposed to the service conditions in their respective locations.

5.7.2 Definition of Equipment Qualification

UK ABWR is designed to provide several reliable levels and protection methods to minimise the probability of Nuclear Power Plant (NPP) accidents, to mitigate their radiological consequences and to prevent the release of radioactive materials. Such reliable protection methods are necessary to ensure that the safety systems and equipment can perform their safety functions when required during Plant Operating conditions which are defined in sub-section 5.7.3.2.

Equipment Qualification (EQ) is defined as the generation and maintenance of evidence to ensure that equipment will operate on demand to meet system performance requirements under specified service conditions including accidental environment (e.g. Loss of Coolant Accident (LOCA), High Energy Line Break (HELB) and seismic or other vibration conditions). EQ demonstrates that equipment designs are capable of performing their own functions under these service conditions.

EQ is an important design tool when safety equipment is qualified to tolerate the conditions that could cause equipment failures.

The EQ process consists of the following steps:

- Identifying safety functions and equipment requiring qualification
- Identifying the set of Plant Operating Conditions existing when the performance of equipment has to be accomplished
- Selecting appropriate qualification methods and implement them, and
- Demonstrate qualification against documented acceptance criteria

5.7.3 Scope of Application for EQ

5.7.3.1 Identifying Safety Functions and Equipment Requiring Qualification

Safety equipment is qualified for the operating conditions when the safety functions of the specific equipment are required.

Safety functions are identified to prevent or reduce the radiological risk for all identified faults and hazards, and they are categorised according to their importance for safety, and equipment that deliver each safety function are identified and assigned a classification based on the importance of

the safety functions they perform. The safety functions, the safety categorisation, and the safety classification of the equipment of UK ABWR which deliver the safety functions are defined in section 5.6.

In principle, the UK ABWR mechanical and electrical equipment and the related structures which have a high safety importance (Safety Class 1 or 2) for delivering High Level Safety Functions are qualified according to the EQ process.

5.7.3.2 Identifying Operating Conditions

Safety equipment has to perform its safety function during normal, abnormal, test, design basis accident and post-accident environments as applicable.

The qualification for Operating Conditions (Operating Condition I, Operating Condition II, Operating Condition III, Operating Condition IV) is necessary to be established and selected so as to provide confidence in equipment performance during expected Operating Conditions.

The expected Plant Operating Conditions are defined in section 5.4 of this chapter.

During EQ, the following service conditions are considered:

- Process related conditions are also considered such as vibration, load cycling, electrical loading parameters, Electromagnetic Interference (EMI), mechanical loads and process fluid conditions (e.g. pressure, temperature, chemistry, cavitation, flow rate).
- Seismic vibration (combined with process vibration) , and
- Environmental conditions such as the ambient temperature, pressure, humidity/steam and radiation.

5.7.3.3 Selecting Appropriate Qualification Methods and Establishing Qualification

The EQ process includes qualification of the initial equipment installation and subsequent requalification or replacement during the life of the plant as appropriate to demonstrate continuous fulfillment of performance requirements.

The methods of qualification are:

1. Performance of a type test on representative equipment to be supplied;
2. Performance of an actual test on the supplied equipment;
3. Application of pertinent past experience in similar applications;
4. Analysis based on reasonable engineering extrapolation of test data or operating experience under pertinent conditions, and
5. An appropriate combination of these four methods.

5.7.4 Qualification Methods for Facilities and SSCs

5.7.4.1 General

Equipment Qualification verifies that equipment with a safety function is operated as expected in the design under environment conditions considered in internal hazard assessment, external hazard assessment and fault studies. Hitachi-GE evaluates the validity and the effectiveness of equipment with a safety function by means of qualification tests, analysis or comparative evaluation of past Japanese qualification data. Test conditions such as environment simulation of severe accidents, postulated accidents, and transient conditions that are specified in internal and external hazard assessments and fault studies. Dynamic loads, static loads and functional requirements for equipment are described in each design specification.
Qualification tests, analysis or evaluation of past qualification data will be compiled in a report after clarifying its qualification method (qualification test/analysis).
The detailed arrangements for Equipment Qualification are described in "Generic Equipment Qualification Guideline [Ref-5.7-1]."

5.7.4.2 Synergistic Effect

Equipment Qualification test conditions are assessed individually as far as possible but only if no significant synergistic effects occur, in order to properly evaluate the impact on the equipment. If synergistic effects caused by interrelated events are assumed, these are identified and considered in the test specification for Equipment Qualification.

5.7.4.3 Mild Environmental Condition

The mild environmental condition refers to locations in the NPP where environmental conditions do not significantly change as a result of Postulated Initiating Events (PIEs), except for seismic events.
Examples include the Main Control Room and electrical panel rooms. Temperature, moisture, and radiation under severe accident conditions are not applied to the Main Control Room, control panels in electrical panel rooms, or racks.

5.7.4.4 ASME B&PV Code Sec. III

Equipment that is not related to dynamic function qualification, such as pressure components and core support structures manufactured in accordance with ASME B&PV Code Sec. III are not subject to qualification tests by analysis since load combinations are taken into account in the design report.

5.7.4.5 IEC/IEEE 60780-323

Equipment Qualification is performed on electrical and instrumentation products in accordance with IEC/IEEE 60780-323. Test items and conditions for each equipment item are specified in the design specification for each equipment item. All or some of the test items is evaluated by analysis or past qualification results.

5.7.4.6 Equipment Qualification

Equipment Qualification on applicable items is planned and carried out considering the 60 year design life or the equipment life specific to the product. The design life is evaluated and verified by qualification tests, analysis or past qualification data. If the design life or the expiration date is set,

requirements for maintenance, surveillance, and periodic test are also specified in order to maintain the integrity of equipment.

The following test specification is considered when performing Equipment Qualification.

(1) Because the influence of magnetic fields, thermal and radiation environments and electromagnetic compatibility (EMC), may impair semiconductor devices in computer based control equipment, testing is performed. The EMC test condition specifies thermal environment and radiation environment, taking into account the environment in Operating Conditions I to IV, based on internal and external hazard assessments and fault studies. In thermal environments, the influence of pressure, temperature, and moisture are considered. EMC is performed to consider the influence of transient, conducted noise, emissions at working site, and resistance to electromagnetic waves.

(2) Product function and function time.
When the operation of equipment with a safety function is verified, the time until its safety function is required and the time that safety function is maintained, are taken into consideration.

(3) Plant events and combination of events based on internal hazards, external hazards and fault studies.
Qualification requirements for significant equipment with safety function need to consider plant events. Specific plant events are considered in equipment specifications and Equipment Qualification procedures for each equipment item. Moreover, if events occur simultaneously or sequentially or may reasonably be expected to do so, appropriately qualified conditions are considered.

5.7.4.7 Qualification of Seismic Loads and Dynamic Loads

Seismic and dynamic qualification for systems and components is performed in terms of structural integrity and functionality. The qualification is in accordance with ASCE 43. The detailed qualification methods are based on ASME Sec. III, ASME NOG-1 and ASME AG-1 for structural integrity, and are based on ASME QME-1, IEC/IEEE 60780-323, IEC 60980, IEEE 344, etc. for functionality.

The principle of seismic and dynamic qualification is to confirm that the capacity of equipment exceeds the bounding demand required by the safety case. The demand of equipment is derived from required response spectrum based on dynamic analysis. The capacity of the equipment is evaluated by test, analysis, experience, data in actual plants, or by a combination of test information and analysis.

5.7.4.8 Qualification Codes and Standards

The codes and standards for Equipment Qualification are as follows:

Qualification for structural integrity

Equipment Name	Qualification Code and Standard
Vessel, incl. Heat Exchanger Piping Pump Reciprocating Pump Valve Dynamic Support Structure	ASME Sec. III Subsection NB, NC, ND
Metal Containments	ASME Sec. III Subsection NE
Support (Dynamic support Structure)	ASME Sec. III Subsection NF
Core Support Structure	ASME Sec. III Subsection NG
Lifting Machine relating Fuel Route	ASME NOG-1
MCR Emergency Ventilation (HVAC)	ASME AG-1

Qualification for functionality

Equipment Name	Qualification Code and Standard
SSCs with dynamic and electrical function • RCIC Turbine • Electric Motor • Fan • Damper • Emergency DG • Pump • Valve • Dynamic Support Structure	ASCE 43 ASME QME-1 IEC/IEEE 60780-323 IEC 60980 (IEEE Std 344) IEEE 382

Qualification for Electric and I&C

Equipment Name	Qualification Code and Standard
Electric parts	IEC 61000-SER IEC/IEEE 60780-323 IEC 60980

5.7.5 Qualification Documentation

Hitachi-GE verifies the condition of environmental, earthquake-proof, and dynamic functions by the application of dynamic loads that are specified in design specifications, and prepares the necessary qualification documentation. Safety functional and other critical characteristics required for products and equipment are clarified, and the relationship between qualification tests, analysis or design evaluation and qualification records make up the qualification documentation. Qualification documentation ensures the traceability of product or installation which is delivered to the nuclear power plant.

5.7.5.1 Qualification Plan

Qualification tests are carried out on equipment with a safety function in accordance with the Qualification Plan. The Qualification Plan states the test procedures, environment and also the equipment to be qualified. Test items are generally determined based on the provision of recommended codes and standards, but for equipment proven in the reference plant; the design department may specify a qualification test, analysis or technical assessment separately at the Design Review.

5.7.5.2 Instructions and Implementation of Qualification Test

Qualification tests are carried out and instructed in accordance with the Qualification Plan. For qualification of equipment with a significant safety function, qualification by a third party inspection agency might be included, depending on the importance of the items requiring qualification.

5.7.5.3 Qualification Test Report

The Qualification test report describes all test results and qualification results. Typical report content is listed below.

(1) Overview of Test Results.
(2) Consideration of Test Results.
(3) Technical Specification in regard to Product Qualification Test.
(4) Specific Conditions and Resolutions, and
(5) Review and approval of Qualification test results. The persons responsible are required to be qualified and approved for the review and approval of Qualification tests.

5.8 Applied Regulations, Codes and Standards

5.8.1 Introduction

This chapter describes the codes and standards applied to the UK ABWR that have been designed and constructed by Hitachi-GE Nuclear Energy, Ltd. in the United Kingdom. Hitachi-GE takes into account the UK regulatory expectations, practices and applicability when adopting codes and standards for the UK ABWR. The UK nuclear safety regulations are based on a non-prescriptive regime and consequently it does not prescribe the technical codes and standards that must be used for nuclear new build. However, the codes and standards must represent good practice and be consistent with the requirements of ALARP. Hitachi-GE has identified the appropriate international and national codes and standards and particularly those that are nuclear-specific, and has applied them to the generic design and shall apply them to the construction of the UK ABWR.

The codes and standards identified in this report cover the following technical areas:

(1) Structural Integrity
(2) Mechanical
(3) Control and Instrumentation (C&I)
(4) Electrical Supplies
(5) Civil Engineering
(6) Resilience to Hazards including Seismic Design and Fire Protection, and
(7) Quality Assurance

For the purpose of GDA a separate report defines the Categorisation of the safety functions and the Classification of Structures Systems and Components of the UK ABWR [Ref-5.1-4]. This section is thus limited to a discussion of international and national codes and standards adopted for Class 1 and 2 SSCs for the UK ABWR. The codes and standards related to manufacturing such as material selection and welding, special process for example heat treatment, and Non Destructive Examination have been provided in GDA.
The wider and detailed description of codes and standards is provided in a "Topic Report on Acts, Regulations, Codes and Standards [Ref-5.1-5]."

5.8.2 Technical Approach

The codes and standards used are selected in accordance with the safety categorisation of the function and safety classification of the SSCs. Appropriate codes and standards for the category and class are evaluated for their applicability, adequacy and sufficiency in this report. Hitachi-GE considers that the applicability of the codes and standards should also be based on their practical experience in the design and construction of the ABWR. Table 5.8-1 provides a summary and comparison of the principal codes and standards adopted for the UK ABWR. These codes and standards are specific to nuclear applications.

Table 5.8-1: Principal Codes and Standards to be adopted for the UK ABWR

Engineering	UK ABWR	Reference ABWR
Structural Integrity	ASME BPVC Sec. III Div.1 ASME BPVC Sec. VIII	JSME S NC-1 JIS
Mechanical	BS, ISO Manufacture's standards	JIS Manufacture's standards
C&I	IEC Nuclear Power Plant	JEM, JIS, JEAC and JEAG
Electrical	IEC Nuclear Power Plant	JEM and JIS
Civil	ASME BPVC Sec. III Div.2 ACI 349 ANSI/AISC N690	JSME S NE-1 JASS 5N AIJ Standards
Seismic	ASCE 4 ASCE 43	JEAC4601
Quality Assurance	GSR Part 2, ISO9001 ASME NQA-1	JEAC4111, ISO9001

To summarise:

- The codes and standards used for design which are discussed here are limited to the Class 1 and 2 SSCs. Although not covered specifically in this chapter the approach is extended to Class 3 SSCs and non-safety standards.

- The equivalence of codes and standards used historically for the ABWR and those used for the UK ABWR is illustrated below:
  - The JSME code is highly compatible with the ASME code as it has its origin in the ASME code dating back to the 1980s.
  - The Japanese Industrial Standards (JIS) are compatible with international standards for example those from the International Electrotechnical Commission.
  - ASME BPVC Sec III is a notable nuclear specific standard for structural integrity and has been applied in UK nuclear reactor design and adopted for the UK ABWR.

- The detailed justification of the approach to the selection and application of the codes and standards to the SSCs is provided in other relevant Generic PCSR chapters where the SSCs are described.

- The selection of codes and standards has been prioritised, for example for electrical engineering IEC standards have priority, but in the absence of a suitable standard, JIS or IEEE standards have been used, particularly when they have been shown to be practical and proven by application for the J-ABWR.

- The combination and mixing of standards from different sources have been avoided to ensure that the standards used are complete and consistent.

The version of the standards applied has been the latest editions with their addenda; the actual versions have been identified during GDA as part of the design reference point. However, where designs have been completed or procurement / engineering practice requires historic versions to be used a gap analysis have been undertaken to demonstrate equivalence. If gaps are found, remedial measures have been identified and applied and this has been done on a case by case basis.

5.8.3 Discipline Specific Codes and Standards

5.8.3.1 Structural Integrity Codes and Standards

Major structural components whose integrity is important to safety are designed in accordance with the ASME Boiler & Pressure Vessel Codes Section III (ASME Sec. III) which is nuclear specific and is recognised internationally.

Table 5.8-2 Structural Integrity Codes and Standards for Class 1 and 2 identifies the major codes and standards to be applied for Class 1 and 2 component types of the UK ABWR. [Ref-5.1-4]

Class 3 components have been designed in accordance with ASME Boiler & Pressure Vessel Codes Section VIII with ISO, European and BS standards also used on some components, and explicitly stated where applied. Piping and valves have been designed in accordance with ANSI/ASME B31.1 and B16.34 to maintain consistency with ASME Sec. III piping. Japanese Codes and Standards which are proven in reference plant may apply to Class 3 components due to availability and for practical reasons. Table 5.8-3 shows that Structural Integrity Codes and Standards which are to be applied to Class 3 component types.

Table 5.8-2: Structural Integrity Codes and Standards for Class 1 and 2

SSCs Type	Applicable Codes and Standards
Pressure Vessel	ASME BPVC Section III, Division 1 ASME BPVC Section II, ASME BPVC Section V, ASME BPVC Section IX, ASME BPVC Section XI
Heat Exchanger	
Storage Tank	
Valve	
Piping	
Pump	
Support	
Reactor Internal	
Reinforced Concrete Containment Vessel	ASME BPVC Section III, Division 1 ASME BPVC Section III, Division 2
Lining Pool	ASME BPVC Section II, ASME BPVC Section V, ASME BPVC Section IX

Table 5.8-3: Structural Integrity Codes and Standards for Class 3

SSCs Type	Applicable Codes and Standards
Pressure vessel	ASME BPVC Section VIII, Division 1and 2
Heat Exchanger	ASME BPVC Section VIII, Division 1and 2 HEI Standards
Piping	ANSI/ASME B31.1 BS EN 13480
Pump	BS EN ISO 13709 Hydraulic Institute Standards BS Pump Manufacturers' Association API 610
Valve	ANSI/ASME B31.1 ANSI/ASME B16.34
Storage Tank	BS EN 14015 API 650 ANSI/ASME B96.1 API Standard 2000

5.8.3.2 Mechanical Codes and Standards

Mechanical equipment is designed in accordance with ISO, BS and European standards in principle. Pumps, diesel engines, lifts etc. are designed ISO standards. However, nuclear specific equipment such as the Fine Motion Control Rod Drives, Hydraulic Control Units and Reactor Internal Pumps are designed to the manufacturer's standards; the design and drawings are required to be justified prior to construction. Table 5.8-4 shows the list of major mechanical codes and standards.

Table 5.8-4: Mechanical Codes and Standards

SSCs Type	Applicable Codes and Standards
Pump	BS EN ISO 13709 Hydraulic Institute Standards BS Pump Manufacturers' Association API 610
Valve	ASME BPVC Sec. III Div. 1 ASME QME-1 IEEE 382
Diesel Engine	ISO 8528 (series) Reciprocating internal combustion engine driven alternating current generating sets
MCR Emergency Ventilation (HVAC)	NVF/DG001 Issue 1 An Aid to the Design of Ventilation of Radioactive Area ASME AG-1
Lifting Machine relating to Fuel Route	ASME NOG-1 BS EN 13001 BS EN 15011

5.8.3.3 C&I Codes and Standards

Control and Instrument equipment is, in principle, designed in accordance with standards produced by International Electrotechnical Commission (IEC) TC45/ SC 45A Nuclear Power Plant standards. These are recognised international nuclear codes and standards and they are applied to new civil nuclear projects in European countries. Table 5.8-5 C&I codes and standards, shows a list of high level C&I codes and standards which have been applied in the design of the UK ABWR.

Table 5.8-5: C&I Codes and Standards

IEC Standards	Title
IEC 61513	Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
IEC 61226	Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions
IEC 62138	Nuclear power plants - Instrumentation and control systems important safety Software aspects for computer - based systems performing category B or C functions
IEC 60987	Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems
IEC 62566	Nuclear power plants - Instrumentation control important to safety - Development of HDL-programmed integrated circuits for systems performing category A function
IEC/IEEE 60780 -323	Nuclear facilities - Electrical equipment important to safety - Qualification Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
IEC 60980	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations
IEEE 344	Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations

5.8.3.4 Electrical Supplies Codes and Standards

Electrical equipment is, in principle, designed and constructed in accordance with IEC standards that are recognized as international codes and standards appropriate for nuclear application in European countries. IEC codes and standards are given priority over the other codes and standards and are available for specific equipment; in the absence of an IEC standard a BS or European standard has been used. Special equipment may use existing codes and standards with justification. Table 5.8-6 Electrical Codes and Standards show the list of major electrical equipment such as control panel, switchgear, motor, generator, transformer, power bus and battery.

Table 5.8-6: Electrical Codes and Standards

Category	Typical Equipment	Applicable Codes and Standards
Control Panel	Main Control Panel Local Control Panel	IEC 60964 IEC 61227 IEC 61839 IEC 61772
Switchgear	Metal-clad Switchgear Power Centre Motor Control Centre	IEC 62271-SER IEC 60947-SER IEC/TR 62271-300 IEC 60038
Motor	High Voltage Induction Motor Low Voltage Induction Motor Direct Current Motor Stepping Motor	IEC 60034-SER
Generator	Main Generator Diesel Engine Generator	IEC 60034-SER
Transformer	Exciter Transformer Service Transformer	IEC 60076-SER IEC 60044-SER IEC 60137
Power Bus	Isolated Phase Bus (IPB) Non-segregated phase Bus	IEC 298
Battery	Battery Battery Rack	IEC 60896-11 IEC 60896-22 IEC 61056

5.8.3.5 Civil Engineering Codes and Standards

The UK ABWR civil structures have been designed in accordance with ASME BPVC Sec. III Division 2 for Reinforced Concrete Containment Vessel and to ACI 349 and ANSI/AISC N690 for other major buildings. These are recognised international codes and standards for civil engineering. Table 5.8-7 Civil Engineering Codes and Standards identify the applicable codes and standards for civil engineering of the UK ABWR. ACI 349 is applied to civil engineering because ACI is consistent with the use of ASME BPVC Sec. III Div. 2, which is the design codes used for the RCCV. The applicable codes and standards have been allocated to each building commensurate with their safety classification. European or British codes and standards may be applied to the buildings that are not related with off-site large scale release of radiation; their use has been identified from safety categorisations and classification of the buildings.

The codes and standards related to construction, test and qualification of civil engineering may use European and BS standards in line with their applicability at a construction site. ISO, EN or BS materials codes and standards have been justified along with the US design codes. This has been provided in later step of GDA and the difference between ISO and US codes and standards has been evaluated and described in these GDA documents.

Table 5.8-7: Civil Engineering Codes and Standards

Codes and standards	Title
ASME BPVC Sec. III Division 2	Rules for Construction of Nuclear Facility Components, Division 2: Code for Concrete Containments
ACI 349	Code Requirements for Nuclear Safety- Related Concrete Structures
ANSI /AISC N690	Specification for Safety-Related Steel Structures for Nuclear Facilities
NUREG-800	USNRC Standard Review Plan for Review of Safety Analysis Report for Nuclear Power Plants- LWR Edition 3.8.1 Concrete Containment 3.8.4 Other Seismic Category I Structures 3.8.5 Foundations
RG 1.136	Design Limits, Loading Combinations, Materials, Construction, and Testing of Concrete Containments

Codes and standards	Title
RG 1.142	Safety-Related Concrete Structures for Nuclear Power Plants (Other than Reactor Vessels and Containments)
ACI 318	Building Code Requirements for Structural Concrete and Commentary

5.8.3.6 Hazards and Conventional Safety Codes and Standards

Codes and standards for hazards and conventional safety related to the UK ABWR have been identified as a part the GDA development process and are described in relevant safety case documents.

5.8.3.7 Seismic Design

The seismic design of the UK ABWR has taken account of the relevant IAEA safety standards. Table 5.8-8 Codes and Standards for Seismic Design identifies the codes and standards for seismic design. Soil investigation and hazard assessment that provide the seismic design conditions are addressed in accordance with IAEA safety standards which are recognised internationally. ASCE nuclear specific standards are applied to the detailed seismic design. The methodology is to apply IAEA standards and ASCE this methodology is described in the initial safety case on Civil Engineering and External Hazards (see Chapters 10: Civil Works and Structures and Chapter 6: External Hazards of this Generic PCSR respectively).
Seismic design codes are described in "Topic Repot on Acts, Regulations, Codes and Standards [Ref-5.1-5]".

Table 5.8-8: Codes and Standards for Seismic Design

Items	Standards
Soil Investigation Seismic Hazard Assessment	IAEA SSG-9 Seismic Hazards in Site Evaluation for Nuclear Installations
	NS-G-3.6 IAEA, Geotechnical Aspects of Site Evaluation and Foundations for Nuclear Power Plants
Seismic Design	ASCE 4 Seismic Analysis of Safety-Related Nuclear Structures and Commentary
	ASCE 43 Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities
	EUR Volume 2 General Nuclear Island Requirements, Chapter 4 Design Basis
Seismic Design Parameter Seismic Systems Analysis Seismic Subsystem Analysis	NUREG-0800 USNRC Standard Review Plan for Review of Safety Analysis Report for Nuclear Power Plants- LWR Edition 3.7.1 Seismic Design Parameters 3.7.2 Seismic System Analysis 3.7.3 Seismic Subsystem Analysis
Damping Values	RG 1.61 Damping Values for Seismic Design of Nuclear Power Plants
Seismic Response Analysis	RG 1.92, Combining Modal Responses and Spatial Components in Seismic Response Analysis

5.8.3.8 Fire Protection Codes and Standards

Fire protection for nuclear safety is designed in accordance with the principles of IAEA NS-G-1.7. The design, and the materials and equipment to be constructed shall be in accordance with British Standards to ensure the consistency with requirements for conventional safety and qualification. British Standards are used in preference to other codes and standards; however, if no appropriate British Standards are available, existing applicable codes and standards may be applied and their use accompanied with a justification.
Fire protection safety requirements are described in "Topic Report on Acts, Regulations, Codes and Standards [Ref-5.1-5]".

Table 5.8-9: Codes and Standards for Fire Protection

Standards	Title
NS-G-1.7	Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants
BS 9990	Code of practice for non-automatic fire-fighting systems in buildings
BS 5306-1	Code of practice for fire extinguishing installations and equipment on premises. Hydrant systems, hose reels and foam inlets.
BS 5306-2	Fire extinguishing installations and equipment on premises. Specification for sprinklers systems
BS 5839-1	Fire detection and fire alarm systems for buildings
BS 476-10	Fire tests on building materials and structures.
BS EN 13501-1	Fire classification of construction products and building elements classification using test data from reaction to fire tests

British Standard 9999, the code of practice for fire safety in the design, management and use of building is not applicable to nuclear licensed plant but is considered as a source of good practice in the design and operation of UK ABWR.

5.8.3.9 Human Factors Engineering Codes and Standards

This section describes Human Factors Engineering (HFE) codes and standards related to the UK ABWR.

HFE design of the UK ABWR applies the IAEA Safety Standards (Requirements and Guides), US NRC NUREG, BS, EN standards, ISO, and IEC standards. Table 5.8-10 shows the list of major HFE codes and standards. A detailed description of HFE codes and standards is provided in the "Topic Report on Acts, Regulations, Codes and Standards [Ref-5.1-5]".

Table 5.8-10: Codes and Standards for Human Factors Engineering

Codes and Standards	Title
UK Ministry of Defence: Defence Standards 00-250	Human Factors for Design of Systems Part 0 Human Factors Integration
IAEA DS-431	Design of Instrumentation and Control Systems for Nuclear Power Plants
US NRC NUREG-0700	Human - System Interface Design Review Guideline
US NRC NUREG-0711	Human Factors Engineering Program Review Model
US NRC NUREG-0899	Guideline for the Preparation of Emergency Operating Procedures
US NRC NUREG-1842	Evaluation of Human Reliability Analysis Method
US NRC NUREG/CR-1287	Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application
US NRC NUREG/CR-3331	A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control
US NRC NUREG/CR-6883	The SPRA-H Human Reliability Analysis Method

5.9 Examination, Maintenance, Inspection and Testing

5.9.1 Introduction

This chapter describes the design approach to examination, maintenance, inspection and testing (EMIT) assigned to Structures, Systems and Components (SSCs) significant to safety.

The primary purpose of EMIT is to provide assurance during the operational phase of the UK ABWR that, in terms of nuclear safety, the UK ABWR design integrity is maintained by demonstration of the functional reliability inherent in the design.

5.9.2 Purpose and Scope

EMIT verifies that performance of SSCs satisfies the safety requirements inherent in the design in accordance with the relevant claims, arguments and evidence presented in the Generic PCSR. Each SSC is examined and/or tested for its conformance with the codes and standards prescribed according to the relevant safety classification. Details of such EMIT will be specified in the Design Specification and in the Quality Plan/Inspection and Test Plan for each SSC.

(1) EMIT is prescribed according to relevant safety class of each SSC. EMIT activities for SSCs classified as A1 and A2 are specified based on the required codes and standards. [Ref-5.1-5]
(2) EMIT may be required to go beyond code compliance (particularly for Very High Integrity (VHI) and High Integrity (HI) components) in order to demonstrate that the SSC performs as necessary.
(3) Details of the SSCs to be subject to EMIT are prescribed in the Quality Plan/Inspection and Test Plan with the specified EMIT items and implementation period.
(4) The Quality Plan/Inspection and Test plan clarifies the test and inspection method, acceptance/rejection criteria, required records and hold points by the future licensee and the details of any independent third party inspection agency (if necessary).
(5) Where technically feasible, Factory Acceptance Tests (FAT) will be completed before components are received and installed.
(6) Where technically feasible, Site Acceptance Tests (SAT) will be test and inspection carried out following installation. However, it is recognised that some SSCs can only be adequately tested, e.g. pressure boundary pipework, once fully installed thereby allowing the test procedure to emulate operational conditions. Accordingly, some testing may be carried out under commissioning control.
(7) The measurement scope, model, accuracy and precision of instrumentation equipment used for testing, inspection and monitoring are specified appropriately.
(8) Within the test procedures control measures are specified to ensure progress to the next step of the EMIT process is prohibited if the previous step has not been completed with acceptable results, and
(9) The type, method, scope and testing result evaluation criteria and schedule for EMIT during the operational phase of the UK ABWR will be defined by the future licensee post GDA.

5.9.3 Examination, Maintenance, Inspection and Testing

5.9.3.1 Manufacture and Work Test (Factory Acceptance Tests)

Required tests and inspections together with the performance verification are carried out at a manufacturer's works before the shipment of an SSC important to safety in accordance with the design, codes and standards. Specific selection of the test items, implementation period and test guidance are defined according to the safety class of the relevant SSC and will be described in the individual Design Specification and Quality Plan/Inspection and Test Plan.

5.9.3.2 On Site Plant Installation, Facility Acceptance Test and Commissioning (Site Acceptance Tests)

(1) Mechanical, Electrical, Control and Instrumentation SSCs at Plant Installation Phase

Testing and Inspection on site verifies any test and inspection items that were not confirmed at the manufacturer's works or those related to the construction work implemented during construction on site. Specific selection of the test items, implementation periods and test guidance are defined according to the safety class of relevant SSCs and will be described in the individual Design Specification and Quality Plan/Inspection and Test Plan.

(2) Test and Inspection of Building and Structure at Plant Installation Phase

Inspection and testing commensurate with the safety class is carried out for the reactor building of the UK ABWR during the construction period followed by periodic inspections during the in-service period.
Specific selection of test items, implementation period and test guidance are defined according to the level of importance of relevant SSCs and will be defined in the Quality Plan/Inspection and Testing Plan. The detail of inspection items will be established during the site specific stage.

(3) Commissioning

The adequacy of construction and installation of SSCs are verified during construction and installation commissioning. Details of the commissioning programme are provided in Generic PCSR Chapter 29: Commissioning.

5.9.3.3 Preventative Maintenance

There are many types of maintenance programmes but two major types are usually specified as follows:

- Corrective Maintenance, i.e. activities carried out after a fault has occurred in order to restore an item to a serviceable state;
- Preventative Maintenance (PM), i.e. systematic and prescribed work undertaken at regular predetermined intervals to:

- Reduce the probability of failure
- Restore inherent level of SSC reliability, and
- Ensure that the SSC is not degraded by time or usage

PM also provides an opportunity to again the important element of operational experience where the feedback to improve PM practices. For the UK ABWR PM is a key factor in the basis for the design of all SSCs important to safety to ensure the minimisation of equipment breakdowns. However, in the unlikely event that a SSC breakdown does occur, then the diagnostics that support it will mean that data will be available so that lessons can be learned from the breakdown. These lessons learned can be used to either take action to either improve the PM practices or to change the operational profile of the SSC. Details of all site related maintenance activities will be provided post GDA by the future licensee. However this section provides a brief overview of PM for the generic design of UK ABWR. Each relevant chapter in this Generic PCSR contains a brief overview of EMIT activities and also references lower tier safety case documents where more detailed information can be found.

PM is described as the primary means of providing high quality EMIT activities for the UK ABWR in the Maintenance Philosophy Document [Ref-5.9-1]. This document is supported by other documents on maintenance and the closely related and the integrated topics of testing, inspection and examination:

(1) Maintenance Strategy Implementation [Ref-5.9-2]
(2) Preparation for Establishing a Condition Management Strategy [Ref-5.9-3]
(3) Equipment Lifecycle Management [Ref-5.9-4]
(4) Preventative Maintenance Review Process [Ref-5.9-5]
(5) Reliability Assurance Programme Overview [Ref-5.9-6], and
(6) Generic Technical Specifications [Ref-5.9-7]

The above documents provide guidance on a wide range of practices based on international (Institute of Nuclear Power Operations) and UK good practice. There are two basic philosophies for PM based EMIT, performance based and condition based.

The main concepts described in [Ref-5.9-1] are based on the following:

(1) **Reduce the probability of failure** – to achieve this the design uses the twin concepts of proof testing and in-service performance monitoring/condition monitoring. Proof testing is primarily applied to back up safety systems normally in a dormant state waiting for a demand. The proof test demonstrates that the system is available should a real time demand occur. Where technically feasible, proof testing emulates the actual fault condition to which the safety function is required for prevention, protection or mitigation.

    UK ABWR safety systems' design supports proof testing of important safety functions, major elements of which can be undertaken during normal operation. A good example of this is the proof test of both the Safety System Logic and Control system (SSLC) (see Gneric PCSR Chapter 14: Control and Instrumentation for more information on the SSLC) and the High Pressure Core Flooder System (HPCF) (see Generic PCSR Chapter 13: Engineered Safety Features for more information on the HPCF). The SSLC is used to routinely support the start-up and full test of the HPCF with the exception of actual injection of water into the reactor. Additionally this proof test, although it needs to be undertaken in the test mode, does not inhibit the safety function of the HPCF under test, i.e. the HPCF remains available in the unlikely event of a genuine demand during testing. Should a genuine safety demand arise then the SSLC will realign the control of the HPCF under test

to ensure that it can deliver its safety function. An important concept employed for proof testing is to have a comprehensive understanding of the extent of the functionality being proof tested. As there are few occasions whereby an 'end-to-end' test of the entire functionality of a safety system is technically feasible under operational conditions, proof tests have been designed to show that where they only prove a portion of the system functionality other proof tests ensure an overlap of safety function coverage across all elements being tested, e.g. sensor/logic/actuated device. Although routine proof tests are performed during normal operations some equipment within SSCs can only be tested during an outage, this typically covers sensors and final actuation device such as valves, fans and pumps.

In addition to proof tests the monitoring and trending of the comprehensive range of plant parameters by systems such as the SSLC provide a systematic and high quality source of information. The design of the C&I systems has provided the future licensee with many thousands of plant parameters. Section 5.9.3.4 of this chapter states that the development of the actual details of the Performance Monitoring from Normal Operational data will be developed by the future licensee.

(2) **Restore inherent level of SSC reliability** – For some items, primarily the actuated devices such as valves, fans and pumps, etc., it is recognised that the probability of failure may increase with time and/or usage. This knowledge can be used to determine a scheduled (time or usage based) restoration task, e.g. overhaul. Scheduled overhaul tasks will be designed to ensure the full scope of the inherent level of reliability is restored.

However, as the design basis of UK ABWR provides the means of detecting early warning of incipient failure from diagnostics, performance monitoring and condition monitoring the anticipated preventative maintenance strategy is that of planning corrective maintenance when such early signs of incipient failure are detected. In this case, the comprehensive data collected via proof tests, performance monitoring and condition monitoring can be used to develop the corrective maintenance task to ensure restoration of the inherent level of reliability once completed. The response to such trends will be developed by the future licensee in the site specific stage. However, the GDA safety case and its multiple support documents referenced above on EMIT demonstrates that the design will deliver high quality information to facilitate the adaptation of the EMIT of any SSC that is suffering from a projected fall in reliability based on trends from plant and system data.

(3) **Ensure that the SSC is not degraded by time or usage** – understanding the impact of the operational profile is an important element of achieving required reliability and longevity of performance of a SSC. The operational profile is the totality of the way in which a system is operated and the environment in which it operates. For example the number of starts and stops of a large motor and the conditions under which tests are undertaken could affect the long term reliability performance of motor. Diesel engine performance over time can be significantly degraded if operated off load and especially on light loads. Even where comprehensive proof tests are undertaken on electronic equipment subtle electrochemical effects can build-up and be difficult to detect without a more extensive off-line test bed analysis of sample circuit cards. Although pre-in-service accelerated ageing of electronics will provide early detection of such subtle effects it is not always possible to fully replicate all aspects of an operational profile under test conditions. Therefore, as a part of the strategy for detecting subtle ageing effects linked to age of equipment, a sample test bed analysis of circuit cards may well be a part of an approach to ensure that effect of time and usage do not lead to an unacceptable degradation in the reliability of the performance of SSCs important to safety. For the generic design the operational profiles of all SSCs have

been defined and have been optimised by using decades of experience. This experience and the use of reliability centred maintenance [Ref-5.9-6] have been considerably enhanced and through the use of the UK ABWR Probabilistic Safety Assessment (PSA) (see Generic PCSR Chapter 25: Probabilistic Safety Assessment for more information on the PSA).

Performance monitoring is a means of assessing plant/equipment health and condition by the collection and trending of plant parameters during normal operations, usually collected during operator rounds, e.g. pressures, temperatures, mass flows, motor currents, etc.

Condition monitoring is the collection and trending of specific early signs of equipment distress, e.g. increasing vibration, temperature, oil condition, etc., thereby prompting recovery action before the equipment fails in-service. There are two objectives for condition monitoring; firstly ensuring the availability of safety equipment by detecting early signs of failure. The second objective is assisting in achieving the required Capacity Factor by detecting early signs of potential failures before an in-service failure results in an unplanned shutdown and/or expensive repair costs.

Unlike performance monitoring, which looks at and analyses normal equipment operating parameters, condition monitoring looks for specific features, which, when compared to features for known normal and probable fault conditions, the equipment's conditions can be estimated. Examples of some condition monitoring techniques are listed as follows (more information is provided in [Ref-5.9-3]):

- Off-line Vibration Analysis
- On-line Vibration Analysis
- Oil Analysis
- Thermography
- Motor Current Signature Analysis (MCSA), and
- Partial Discharge Monitoring.

Specific condition monitoring will be determined by the future licensee but the generic design facilitates this approach by providing suitable design features, examples of which are as follows:

- Adequate access for data gathering and inspection;
- Adequate plant operating parameter indication and trending, e.g. power, pressure, temperature, flow, flux etc.;
- Sufficient lubrication and oil sampling points;
- Fixed vibration monitors;
- Thermography windows installed in Electrical Switchgear, and
- Magnetic chip installation especially for rotating plant.

Part of the development of applicable and effective PM routines is the use of a Reliability- centred Maintenance (RCM) methodology. Information on this can be found in the Reliability Assurance Programme document [Ref-5.9-6] and its key inputs are:

- Component criticality assessment;
- PSA;
- EPRI Preventative Maintenance Templates, and
- Legislative requirements, e.g. Lifting Operations and Lifting Equipment Regulations.

The key steps taken in this generic design phase are:

- For each safety important SSC identify applicable and effective PM routines, including where appropriate periodic testing of systems important to safety.
- Categorise each routine as:
  - Generic Technical Specification Surveillance Requirement [Ref-5.9-7];
  - Legislative requirement (see information below on non-RCM);
  - Routine Preventative Maintenance:
    - Performance monitoring:
    - Condition Monitoring;
    - Invasive restoration (e.g. overhaul during an outage, see section 5.9.3.5 of this chapter);
    - Replacement, and
    - Failure-finding task.

However although RCM is an important element of PM it is not appropriate in all cases and has not been applied to:

- Equipment where the maintenance strategy justifies a specific PM programme e.g. In-service Inspection (ISI) or material sampling;
- Equipment subject to prevalent regulations, e.g. Lifting Operations and Lifting Equipment Regulations, Pressure Systems Safety Regulations, etc.;
- Large primary or secondary components, or specific equipment for which the RCM method is not relevant, e.g. turbines, and
- Civil structures.

Information on the above are covered in topic specific safety case documents.

5.9.3.4 Operations (Data Acquisition during Operation)

EMIT activities during normal operation will be developed and detailed in the site specific stage.

5.9.3.5 Outages

A nuclear reactor and its auxiliary facilities have periodic planned outages to carry out maintenance and inspection in order to confirm the soundness of the SSCs that are important to safety, to prevent occurrence or escalation of accidents or failures, and to enable safe and stable operation of the plant. Tasks carried out during outages are as follows;

(1) Confirmation of operational performance and important parameters for the main SSCs.
(2) Confirmation of the soundness of the SSCs through overhaul, inspection and leakage testing.
(3) Periodical change of consumable supplies.
(4) Implementation of measures to identify effects of aging.
(5) Implementation of measures for early identification of abnormalities.
(6) Inspection of SSCs and implementation of measures derived from OPEX at other power stations, and
(7) Replacement of Spent Fuel with New Fuel.

The details of the EMIT to be carried out during an outage are defined in the Quality Plan/Inspection and Test Plan. The details of inspection will be established during the site specific stage.

(1) Overhaul and care
Periodic overhaul and checking is carried out by disassembling and thoroughly inspecting each part visually in order to assess its integrity in terms of aging of the SSCs, together with replacement of the consumables such as lubricants, gaskets and O-rings.
Consumables are replaced according to the maintenance plan.

(2) In-Service Inspection (ISI)
In-service inspection is planned systematically to confirm the soundness mainly in terms of the aging of welded parts of equipment and piping by carrying out relevant non-destructive testing. The scope, method, evaluation criteria, examiners' qualification, records and report of the ISI of the UK ABWR components (including vessels, piping, pumps, valves, bolts and their supporting structures) are provided in accordance with ASME Code Section XI. Detailed procedures for the scope for inspection and testing, the inspection and testing schedule, and its frequency will be defined in the Quality Plan/Inspection and Test Plan. The details of inspection will be established during the site specific stage.

(3) Calibration and Characteristics Tests
Output calibration and characteristics tests are carried out on the electrical and control and instrumentation systems in order to confirm their soundness and to adjust for any drift.

(4) Functional Test
As examination, maintenance, and inspections activities are completed, testing will be performed to verify functionality of the relevant SSCs prior to return to service.

5.9.4 Inspection Requirements

5.9.4.1 General Terms

Test and inspection carried out in the UK ABWR conforms to the requirements prescribed in the Design Specification and Quality Plan/Inspection and Test Plan. The requirements for test and inspection of SSCs are prescribed and carried out in order to verify the safety function, soundness and reliability of the nuclear power plant.

5.9.4.2 Requirements for Test and Inspection

Evaluation and judgment of the results of test and inspection are required to comply with the requirements defined in laws, regulations, codes and standards and Design Descriptions, etc.

Examples of the relevant laws, regulations, codes and standards are indicated below. Specific codes and standards applied to each SSC are listed in section 5.8 of this chapter and the Topic Report on Acts, Regulations, Codes and Standards [Ref-5.1-5].

(1) Laws and Regulations
- See [Ref-5.1-5]

(2) Codes and Standards (Representative examples)
- ASME Section III (Material, Design, Fabrication, Examination, Testing)
- ASME Section V (Non-Destructive Examination)
- ASME Section IX (Welding)
- ASME Section XI (In-service Inspection)
- ASME QME-1 (Qualification for Active Mechanical Equipment)
- IEC 62271-SER (Switchgear)
- IEC 60034-SER (Motor, Generator)
- IEC 60076-SER (Transformer)
- IEC 60896-SER (Battery)
- IEC/IEEE 60780-323 (Electrical equipment of the safety system - Qualification)
- IEC 60980 (Seismic qualification of electrical equipment of safety system), and
- etc.

(3) Design Description

(4) Agreement

(5) Procurement Specification, and

(6) Others

Specific test requirements for each SSC are prescribed in accordance with the relevant Quality Plan/Inspection and Test Plan.

5.10 Conclusions

This chapter provides the general approach to design and outlines high level design principles and definitions based on the Hitachi-GE Nuclear Safety and Environmental Design Principles (NSEDP). The principles and definitions described in this chapter are used throughout the other chapters in this Generic PCSR and its supporting references. Since the specific application of the generic principles presented in this chapter is described in other Generic PCSR chapters that have their own conclusions, there are no requirements for any conclusions to this generic chapter.

5.11 References

[Ref 5.1-1] Hitachi-GE Nuclear Energy, Ltd., “UK ABWR Nuclear Safety and Environmental Design Principles (NSEDPs)” GA10-0511-0011-00001(XD-GD-0046), Rev.1, July 2017

[Ref 5.1-2] ONR, “Safety Assessment Principles (SAPs)-2014 edition” , Rev.0, November 2014

[Ref 5.1-3] Hitachi-GE Nuclear Energy, Ltd., “OPEX Report for UK ABWR” GA91-9201-0003-00698(XE-GD-0419), Rev.5, July 2017

[Ref 5.1-4] Hitachi-GE Nuclear Energy, Ltd., “List of Safety Category and Class for UK ABWR”, GA91-9201-0003-00266(AE-GD-0224), Rev.4, August 2017

[Ref 5.1-5] Hitachi-GE Nuclear Energy, Ltd., “Topic Report on Acts, Regulations, Codes and Standards”, GA91-9201-0001-00128(QGI-GD-0014), Rev.1, August 2017

[Ref 5.1-6] Hitachi-GE Nuclear Energy, Ltd., “Topic Report on Fault Assessment”, GA91-9201-0001-00022 (UE-GD-0071), Rev.6, July 2017

[Ref 5.1-7] Hitachi-GE Nuclear Energy, Ltd., “Topic Report on Safety Requirements for Mechanical SSCs”, GA91-9201-0001-00117 (SE-GD-0308), Rev.2, May 2017

[Ref 5.3-1] Hitachi-GE Nuclear Energy, Ltd., “Human-Based Safety Claims Report”, GA91-9201-0001-00043 （HFE-GD-0064） Rev D, July. 2017

[Ref-5.6-1] International Electrotechnical Commission (IEC), "Nuclear power plants Instrumentation and control important to safety. Classification of instrumentation and control functions", IEC 61226:2009, July 2009

[Ref-5.6-2] IAEA, "Safety of Nuclear Power Plants: Design, Specific Safety requirements", No. SSR-2/1, February 2012

[Ref-5.6-3] IAEA, "Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide", No. SSG-30, May 2014

[Ref-5.6-4] Hitachi-GE Nuclear Energy, Ltd., " GDA Safety Case Development Manual", GA10-0511-0006-00001 (XD-GD-0036), Rev.3, June 2017

[Ref-5.6-5] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Compliance of UK ABWR Design with Nuclear Safety and Environmental Principles (NSEDPS)", GA91-9201-0001-00269 (XE-GD-0743), Rev.0, July 2017

[Ref-5.7-1] Hitachi-GE Nuclear Energy, Ltd., “Generic Equipment Qualification Guideline”, GA91-9201-0003-00672 (QGI-GD-0013) Rev. 0, July 2015

[Ref 5.9-1] Hitachi-GE Nuclear Energy, Ltd., “Maintenance Philosophy”, GA91-9201-0003-01498 (XE-GD-0613) Rev. B, July 2017

[Ref-5.9-2] Hitachi-GE Nuclear Energy, Ltd., “Maintenance Strategy Implementation”, GA91-9201-0003-01501 (XE-GD-0615) Rev. A, September 2016

[Ref-5.9-3] Hitachi-GE Nuclear Energy, Ltd., "Preparation for Establishing a Condition Management Strategy", GA91-9201-0003-01500 (XE-GD-0616) Rev. A, September 2016

[Ref-5.9-4] Hitachi-GE Nuclear Energy, Ltd, "Equipment Life-cycle Management", GA91-9201-0003-01497 (XE-GD-0619), Rev.A, September 2016

[Ref-5.9-5] Hitachi-GE Nuclear Energy, Ltd., "Preventive Maintenance Review Process", GA91-9201-0003-01496 (XE-GD-0620) Rev. A, September 2016

[Ref-5.9-6] Hitachi-GE Nuclear Energy, Ltd., "Reliability Assurance Programme Overview", GA91-9201-0003-01502 (XE-GD-0614) Rev. A, September 2016

[Ref-5.9-7] Hitachi-GE Nuclear Energy, Ltd., "Generic Technical Specifications", GA80-1502-0002-00001 (SE-GD-0378) Rev. 3, August 2017