Form10/00

UK ABWR

HITACHI

Document ID	:	GA91-9901-0007-00001
Document Number	:	XE-GD-0104
Revision Number	:	B

UK ABWR Generic Design Assessment

Categorisation and Classification of Structures, Systems and Components

Hitachi-GE Nuclear Energy, Ltd.

Form10/00

UK ABWR

HITACHI

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

No part of this document may be reproduced in any form, without the prior written permission of Hitachi-GE Nuclear Energy Ltd.

Copyright (C) 2014 Hitachi-GE Nuclear Energy, Ltd. All Rights Reserved.

Hitachi-GE Nuclear Energy, Ltd.

Table of Contents

1. Purpose of Classification 1

2. Safety Function and Categorisation 3
   2.1 Faults, Events, and Safety Functions 3
   2.2 ABWR Safety Functions 3
   2.3 Categorisation of Safety Functions 8

3. Classification 10
   3.1 Safety Classification 10
   3.2 UK ABWR Safety Classes 11
   3.3 Classification and PSA Feedback 13

4. Application of Safety Classes 14

5. Summary of UK ABWR Classification 16

Acronyms

ADS:	Automatic Depressurization System
ALARP:	As Low As Reasonably Achievable
ARI:	Alternative Rod Insertion
BAT:	Best Available Technology /Best Available Techniques
BDB:	Beyond Design Basis
BDBA:	Beyond Design Basis Accident
BDBE:	Beyond Design Basis Event
BSL:	Basic Safety Level
BSO:	Basic Safety Objective
DB:	Design BasisDBE: Design Basis Event
EMIT:	Examination, Maintenance, Inspection and Testing
GDA:	Generic Design Assessment
HPCF:	High Pressure Core Flooder System
HSE:	UK Health and Safety Executive
IAEA:	International Atomic Energy Agency
IEC:	International Electro technical Commission
LPFL:	Low Pressure Flooder System
MS:	Mitigation System
MSIV:	Main Steam Isolation Valve
NPP:	Nuclear Power Plant
PCSR:	Pre-Construction Safety Report
PS:	Prevention Safety functions
PSA:	Probabilistic Safety Assessment
RAW:	Risk Achievement Worth
RPV:	Reactor Pressure Vessel
RPT:	Recirculation Pump Trip
SAP:	HSE Safety Assessment Principle
SSC:	Structures, Systems and Components

This document has been prepared as step 1 document on the categorisation of safety functions and the classification of structures, systems, and components, in general design assessment of the UK ABWR design. This document covers purpose, method, and example of classification, including safety function and lower level functions of UK ABWR

1. Purpose of Classification

The safety of plant is assured by several layers of protection strategy. In a protection strategy, Structures, Systems, and Components (SSCs) that deliver safety functions, have important roles to achieve safety. Furthermore, it is important that SSCs, including software for instrumentation and control, that implement this strategy, should be treated according to their safety significance to assure their reliability and capability effectively. That is, SSCs with safety functions are so designed that the facility‟s safety will be ensured and maintained. The resulting classification of the SSCs that make up the design of a nuclear plant indicates 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 process is an important step in the 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 aim of the safety design is to make the resulting plant tolerant to faults. The process therefore starts with the systematic and comprehensive identification of faults and their categorisation according to their potential consequences and frequency. 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. 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). These safety measures are designed and operated using codes, standards and procedures commensurate with their importance for safety as expressed in their safety classification. Finally, deterministic and probabilistic safety assessments demonstrate that the resulting design meets all the SAP risk targets and reduces risks so far as is reasonably practicable [Ref-1].

The classification approach has been prepared, considering the SAPs (HSE Safety Assessment Principles)[Ref-2], IEC [Ref-3], and IAEA standard [Ref-4]. The steps in the classification approach are described below:

(1) Identify safety functions and assign categories based on their importance to safety.

(2) Identify SSCs that deliver each safety function and assign a classification based on the importance of the safety functions they perform.

(3) Link the classification to a set of requirements for design, construction, and operation, which will ensure that components are at the appropriate level of quality.

The structure of the chapter is as follows:

Chapter 2 describes the first step of methodology, the types of safety functions, and how they are categorised.

Chapter 3 defines the classification approach applied to SSCs that deliver the respective safety functions.

Chapter 4 explains how the safety classification is linked to design requirements for the components.

Chapter 5 describes the summary of UK ABWR classification example.

2. Safety Function and Categorisation

This chapter describes the ABWR safety functions and categorisation of those safety functions.

2.1 Faults, Events, and Safety Functions

Based on SAPs, all faults and events fall into the categories shown in Table 2.1-1below according to the initiating fault/event frequency and the corresponding potential consequences, that is, offsite/onsite radioactive dose.

Table 2.1-1 Faults and Events Categories

[

This information is removed intentionally

]

For each event, it is necessary to identify what needs to be done to reduce the risk to acceptable levels.

There are two principal ways of reducing risk from faults: by preventing the fault from occurring; or by mitigating the fault consequences.

[

This information is removed intentionally

]

Both safety functions that prevent faults and those that mitigate consequences are related to the three fundamental safety functions identified by IAEA: control of reactivity, cooling and containment:

(i) Control of reactivity,
(ii) Removal of heat from the reactor and from the fuel store, and
(iii) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

2.2 ABWR Safety Functions

In this sub-chapter, ABWR safety functions are derived systematically.

The Safety functions in ABWR have been developed from two major safety category groups. One is the group of safety functions whose failure could cause abnormal conditions at nuclear reactor facilities, thereby leading to undue radiation exposure to the public or site personnel. These are designated as abnormality prevention safety functions (PS) in the Japanese practice [Ref-5]. Abnormality prevention functions in ABWR are shown in Table 2.2-1.

The other group contains those whose function is to prevent, in case of abnormal conditions at nuclear reactor facilities, an escalation of such condition or put such conditions under control immediately, thereby mitigating possible radiation exposure to the public or site personnel. These are designated as abnormality mitigation safety functions (MS) in the Japanese practice. Abnormality mitigation functions in ABWR are shown in Table 2.2-2

The identified safety functions also identified with one of the three high-level safety functions, which are similar to fundamental safety functions:

(1) Control of reactivity,
(2) Fuel cooling, and
(3) Long term heat removal

A list of UK ABWR plant level safety functions identified from the Japanese safety case is shown in Table 2.2-3 along with their Japanese classification. These safety functions will be confirmed during the fault studies performed as part of GDA.

Table 2.2-1 Safety function configuration in UK ABWR

(Abnormality Prevention System)

No	Lower level category group	High level safety functions
1	SSCs whose damage or failure could cause events leading to: (a) considerable core damage, or (b) significant fuel failures	Functions to form reactor coolant pressure boundary
		Functions to prevent excessive reactivity insertion
		Functions to maintain core geometry
2	SSCs whose damage or failure could cause events, without considerable core damage or significant fuel failures leading to excessive release of radioactive materials to the off-site areas.	Functions to contain reactor coolant (Except for : small-diameter pipes excluded from the reactor coolant pressure boundary such as instrumentation pipes; other pipes and equipment which are not directly connected to the boundary)
		Functions to store radioactive materials, without direct connections to the reactor coolant pressure boundary
		Functions to handle fuel safely
3	SSCs which are required to function during normal operation and anticipated operational occurrences and whose failure could lead to degraded core cooling.	Functions to reseat safety valves and relief valves
4	SSCs which are not part of above group and whose failure could become initiating events of abnormal conditions.	Functions to retain reactor coolant (other than above)
		Functions to circulate reactor coolant
		Functions to store radioactive materials
		Functions to supply electric power (except for emergency supply)
		Functions for plant instrumentation and control (except for safety protection function)
		Auxiliary functions for plant operation
5	SSCs capable of controlling the concentration of radioactive materials in reactor coolant as low as acceptable for normal operation.	Functions to prevent the dispersion of fission products into reactor coolant
		Functions to clean up reactor coolant

Table 2.2-2 Safety function configuration in UK ABWR

(Abnormality Mitigation System)

No	Lower level category group	High level safety functions
1	SSCs capable of urgently shutting down the reactor, removing residual heat and preventing overpressure within the reactor coolant pressure boundary in the event of abnormal conditions, thereby preventing undue radiological influence on the off-site public.	Emergency shutdown of the reactor
		Functions to maintain sub-criticality
		Functions to prevent overpressure within the reactor coolant pressure boundary
		Functions to remove residual heat after shutdown
		Functions to cool reactor core
		Functions to confine radioactive materials, shield radiation, and reduce radioactive release
2	Other SSCs essential to above safety group.	Functions to generate actuation signals for the engineered safety features and reactor shutdown system.
		Supporting functions especially important to safety.
3	SSCs capable of sufficiently reducing radiological influence on the off-site public in case of damages or failures of category group as follows. Table 2.1-1 No.2 and No.3	Functions to make up water for fuel storage pool
		Functions to prevent radioactive materials release
4	SSCs especially important to cope with abnormal conditions.	Functions to monitor plant conditions in case of an accident
		Functions to mitigate abnormal conditions
		Functions to shut down safely from outside the control room
5	SSCs capable of mitigating anticipated operational occurrences in conjunction with above group.	Functions to mitigate reactor pressure increase with other system
		Functions to suppress reactor power increase with other system
		Functions to make up reactor coolant with other system
6	SSCs required to cope with abnormal conditions.	Functions important to emergency measures and monitoring of abnormal conditions
7	Alternative functions for above functions	Function of alternative reactivity control
		Function of alternative fuel cooling
		Function of alternative containment cooling and decay heat removal
		Function of alternative supporting system

Table 2.2-3 High level safety functions in UK ABWR

Fundamental Safety Function	No	High Level Safety Function	Note (PS/MS)
1. Control of Reactivity	1-1	Functions to prevent excessive reactivity insertion	PS
	1-2	Functions to maintain core geometry	PS
	1-3	Emergency shutdown of the reactor	MS
	1-4	Functions to maintain sub-criticality	MS
	1-5	Functions to circulate reactor coolant	PS
	1-6	Function of alternative reactivity control	-
2. Fuel Cooling	2-1	Functions to form reactor coolant pressure boundary	PS
	2-2	Functions to prevent overpressure within the reactor coolant pressure boundary	MS
	2-3	Functions to cool reactor core	MS
	2-4	Functions to contain reactor coolant (Except for: small-diameter pipes excluded from the reactor coolant pressure boundary such as instrumentation pipes; other pipes and equipment which are not directly connected to the boundary)	PS
	2-5	Functions to store radioactive materials, without direct connections to the reactor coolant pressure boundary	PS
	2-6	Functions to handle fuel safely	PS
	2-7	Functions to reseat safety valves and relief valves	PS
	2-8	Functions to make up water for fuel storage pool	PS
	2-9	Functions to retain reactor coolant (other than above)	PS
	2-10	Functions to store radioactive materials	PS
	2-11	Functions to mitigate reactor pressure increase with other system	MS
	2-12	Functions to suppress reactor power increase with other system	MS
	2-13	Functions to make up reactor coolant with other system	MS
	2-14	Function of alternative fuel cooling	-
3. Long term heat removal	3-1	Functions to remove residual heat after shutdown	MS
	3-2	Functions to confine radioactive materials, shield radiation, and reduce radioactive release	MS
	3-3	Functions to prevent radioactive materials release	MS
	3-4	Functions to prevent the dispersion of fission products into reactor coolant	PS
	3-5	Functions to clean up reactor coolant	PS
	3-6	Function of alternative containment cooling and decay heat removal	
4. Others	4-1	Functions to generate actuation signals for the engineered safety features and reactor shutdown system	MS
	4-2	Supporting functions especially important to safety	MS
	4-3	Functions to monitor plant conditions in case of an accident	MS
	4-4	Functions to mitigate abnormal conditions	MS
	4-5	Functions to shut down safely from outside the control room	MS
	4-6	Functions to supply electric power (except for emergency supply)	PS
	4-7	Functions for plant instrumentation and control (except for safety protection function)	PS
	4-8	Auxiliary functions for plant operation	PS
	4-9	Functions important to emergency measures and monitoring of abnormal conditions	MS
	4-10	Function of alternative supporting system	-

Note: The PS and MS classifications relate to Japanese practice rather than the UK safety case – see Section 2.2.

2.3 Categorisation of Safety Functions

The approach to categorisation and classification of nuclear plant is based on the radiological consequences (risks) of faults and events.

Consequences that are greater than the BSL and with initiating fault frequency > 10^{-5} /year, that is, those in the design basis (DB) region are deemed to be intolerable and must be removed by design, by identifying safety functions that either prevent the failure that leads to the risk or reduce the risk to 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} /year (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 reasonably practicable means of (further) preventing or of reducing them.

Consequences 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 deemed to be part of normal operation. However, such risks are still subject to ALARP 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.

The SAPs (SAP ECS.1) recommend three categories of safety function, determined as follows:

(1) Category A - any function that plays a principal role in ensuring nuclear safety
(2) Category B - any function that makes a significant contribution to nuclear safety
(3) Category C - any other safety function

To categorise safety functions, following factors are taken into account.

a) The consequence of failing to deliver the safety function;
b) The extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;
c) The potential for a functional failure to initiate a fault or exacerbate the consequence of an existing fault;

These three categories are identified with the three risk ranges identified above. The categorisation and classification to be applied to UK ABWR is therefore based on the following identification:

[

This information is removed intentionally

This information is removed intentionally

]

3. Classification

This chapter describes the classification of those safety functions in UK ABWR.

The Safety Measures or Structures, Systems and Components (SSCs) which deliver the Plant Level 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.

3.1 Safety Classification

SSCs that have to deliver safety functions are identified and classified on the basis of those functions and their significance with regard to safety. A safety classification scheme is determined on the following basis:

a) Class 1 - any structure, system, or component that forms a principal means of fulfilling a Category A safety function
b) 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
c) Class 3 - any other structure, system, or components

To classify SSCs, following factors are taken into account.

1) The category of safety functions to be performed by the item;
2) Whether the item is the main or first line provision of the associated safety function or whether the item is a backup or second line provision of the associated safety function.

Other considerations on classification are shown below.

- Auxiliary services that support components of a system important safety should be considered part of that system and should be classified accordingly, unless failure does not prejudice successful delivery of the safety function. These are treated as follows:

  - Supporting systems directly needed for a competent system to fulfill its safety functions are considered to have the class equivalent to that of competent systems.
  - Supporting systems needed for a competent system to maintain or assure its reliability but not directly needed to fulfill its safety functions are considered to have the importance that may be lower than that of competent systems. However, supporting systems for a competent system of class 3 are a minimum of class 3.

- Appropriately designed interfaces should be provided between SSCs of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class. 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 equivalent to higher class shall be considered 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.
- [This information is removed intentionally]

The classification scheme to be implemented for UK ABWR is shown in Table 3.1-1.

Table 3.1-1 : Definition of Safety Classes

Class 1	Any SSC that provides a main or first line means of fulfilling a Category A safety function.
Class 2	Any SSC that provides a backup or second line means of fulfilling a Category A safety function, or provides the main means of fulfilling a Category B safety function.
Class 3	Any SSC that provides a Category C safety function. [This information is removed intentionally]

3.2 UK ABWR Safety Classes

The classification is also a top-down process in each category, starting with the review of higher class.

(1) Class 1
SSCs in Class 1 form principal means of fulfilling a Category A function.

Function to cool reactor core is one of the Category A functions, which will be called upon at infrequent faults and have short time to initiate.[

This information is removed intentionally

]

(2) Class 2
SSCs in Class 2 provide second line or backup means of delivering a Category A safety function, or provide a first line means of ensuring a Category B function.

[
This information is removed intentionally
]

(3) Class 3
SSCs in Class 3 are those providing means of fulfilling category C safety functions. They have safety importance but do not fulfill the requirements for class 1 or class 2. [

This information is removed intentionally

This information is removed intentionally

]

3.3 Classification and PSA Feedback

The initial classification is developed using a deterministic approach, including engineering judgment. After development of classification and design, it is complemented using input from the PSA. In practice, the probabilistic review will be conducted to assess the importance of SSCs. In this process, probability of failure or importance measures, such as Risk Achievement Worth (RAW), may be applied. As a result of this process, the classification may be revised.

4. Application of Safety Classes

This classification reflects a comprehensive view as to how individual safety functions play their role in the overall safety of the plant. According to the importance of SSCs, codes and standards are adopted. However, there are different considerations with respect to specific aspects of SSCs and for specific types of events.

(1) Codes and Standards
Appropriate codes and standards are adopted for SSCs in Classes 1 and 2. If there are no appropriate codes and standards, an approach derived from equivalent codes and standards may be applied. For SSCs in Class 3, appropriate non-nuclear-specific codes and standards may be applied.
Details of codes and standards to be adopted for UK ABWR are given in the document, “Codes and Standards Report” [Ref-6].

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

This information is removed intentionally

]

(3) Seismic Design
The seismic design of the NPP provides mitigation in relation to radiological hazards by maintaining the integrity of SSCs during and after an earthquake. Therefore, the seismic category that corresponds to radiological dose (off-site consequences) is defined, and the integrity of SSCs is evaluated by use of seismic conditions corresponding to each seismic category. The details are as follows:

i. Seismic Category 1: SSCs whose failure would lead to off-site dose > 10mSv and which must therefore confirm integrity during and after DBE*.

ii. Seismic Category 2: SSCs whose failure would lead to off-site dose > 0.01mSv and which is therefore designed to confirm integrity during and after 10^{-3}/year earthquake*.

iii. Seismic Category 3: SSCs whose failure would lead to off-site dose < 0.01mSv and required for operation. They are designed to normal industrial seismic design standards.

* DBE and 10^{-3}/year earthquake are defined in the document, “Preliminary Safety Report on Civil Engineering and External Hazard” [Ref-7].

In addition, SSCs that are not classified as the highest seismic category (Seismic Category 1) but which satisfiy the following conditions are classified as Seismic Category 1A.

- SSCs whose failure could lead to the failure of an adjacent Seismic Category 1 SSC;
- SSCs whose functions are needed to mitigate BDBA after an earthquake or other hazard events.

Furthermore, the details for the seismic categorisation and seismic design motions are described in the document, “Preliminary Safety Report on Civil Engineering and External Hazard” [Ref-7].

(4) Structural Design
Components and structures are assigned as Safety Class 1 to 3 in accordance with the process detailed previously. There are some components that are special cases of Class 1 because there is no reasonably practicable means of adequately mitigating their failure.

These special cases should be 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.

These special components and structures are classified as "Very High Integrity" and the remained are classified as "Standard Class 1". In addition to these, "High Integrity" as intermediate class is considered if applicable. Detail of this is described in document, "Preliminary Safety Report on Structural Integrity" [Ref-8].

For "Very High Integrity" components and structures, the safety case should be especially robust and the corresponding assessment.

An example of the „Very High Integrity" component would be considering the safety case for a steel Reactor Pressure Vessel (RPV). The RPV"s Major Boundary Portion like Shell, Top Head, Bottom Head, Nozzles and so on 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 modelling. 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.

A methodology of identification of „Very High Integrity" components and structures are described in the document, "Preliminary Safety Report on Structural Integrity" [Ref-8]. When this identification is performed, it will be reported in the PCSR and supporting documents.

5. Summary of UK ABWR Classification

This document describes purpose, method, and example of classification of SSCs, in general design assessment of the UK ABWR design. The following table presents the example of classification of safety functions, based on the method in this document. No. 1, 2, and 3 groups of this table show functions related to "Control of reactivity" function, "Fuel cooling" function, "Long term heat removal" function, respectively. No.4 in this table shows functions related to others. These classifications in Table 5-1 are indicative and will be confirmed by fault studies to be carried out during GDA.

Reference

[Ref-1] "Fault Studies to Discuss Deterministic Analysis, PSA and Fault Schedule Development", GA91-9901-0009-00001 Rev.C (XE-GD-0105 Rev.C).

[Ref-2] Health and Safety Executive, "Safety Assessment Principles for Nuclear Facilities " (2006 Edition, Revision 1)

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

[Ref-4] IAEA, "Safety of Nuclear Power Plants: Design", Specific Safety requirements, No. SSR-2/1, 2012.

[Ref-5] The Nuclear Safety Commission of Japan, "NSCRG: L-DS -I.01 Regulatory Guide for Reviewing Classification of importance of Safety Function of Light Water Nuclear Power Reactor Facilities", 1990. http://www.nsr.go.jp/archive/nsc/NSCenglish/guides/lwr/L-DS-I_01.pdf

[Ref-6] "Codes and Standards Report", GA91-9901-0008-00001 Rev.C (XE-GD-0103 Rev.C).

[Ref-7] "Preliminary Safety Report on Civil Engineering and External Hazard", GA91-9901-0004-00001 Rev.B (XE-GD-0112 Rev.B).

[Ref-8] "Preliminary Safety Report on Structure Integrity", GA91-9901-0005-00001 Rev.C (XE-GD-0113 Rev.C).

Table 5-1 Indicative Classification of safety functions (Note: all classifications will be confirmed by fault studies)

[

This information is removed intentionally

]

Table 5-1 Indicative Classification of safety functions (Note: all classifications will be confirmed by fault studies)

[

This information is removed intentionally

]

Table 5-1 Indicative Classification of safety functions
(Note: all classifications will be confirmed by fault studies)

[

This information is removed intentionally

]

Table 5-1 Indicative Classification of safety functions
(Note: all classifications will be confirmed by fault studies)

[

This information is removed intentionally

]

Table 5-1 Indicative Classification of safety functions
(Note: all classifications will be confirmed by fault studies)

[

This information is removed intentionally

]

Table 5-1 Indicative Classification of safety functions
(Note: all classifications will be confirmed by fault studies)

[

This information is removed intentionally

]