Form10/00

HITACHI

UK ABWR

Document ID	:	GA10-9101-0101-05004
Document Number	:	AE-GD-0169
Revision Number	:	A

UK ABWR Generic Design Assessment

Generic PCSR Sub-chapter 5.4 : Categorisation and Classification of Structures, Systems and Components (SSCs)

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

5.4 Categorisation and Classification of Structures, Systems and Components (SSCs)

5.4.1 Purpose of Classification 5.4-1
5.4.2 ABWR Safety Functions.....5.4-3
5.4.3 Categorisation of Safety Functions.....5.4-5
5.4.4 Structures, Systems and Components Important for Safety and their Classification.....5.4-7
5.4.5 Application of Safety Classes 5.4-9
5.4.6 References 5.4-11

5.4 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 is an important part of the development of safety cases. This section covers the purpose and methodology for categorisation and classification used in the UK ABWR safety case.

5.4.1 Purpose of Classification

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. These safety functions are identified by analysis of the causes and consequences of plant failures and categorised according to their importance to the overall safety of the plant and 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 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 process of categorisation starts with the systematic and comprehensive identification of faults and their categorisation according to their potential consequences and frequency as described in Section 5.3. 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.

Both safety functions that prevent faults and those that mitigate consequences are related to the three generic 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 generic 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 proposed for the UK ABWR and is based on guidance given in the HSE Safety Assessment Principles (Ref 1), by the International Electrotechnical Commission (Ref 2) and in IAEA Standards (Ref 3).

5.4.2 ABWR Safety Functions

The Safety Functions in ABWR have been developed systematically 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. 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 reactor facilities thereby mitigating possible radiation exposure to the public or site personnel.

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

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

In addition to these, there are a number of other safety functions designated as “others”.

A list of representative UK ABWR plant level safety functions identified from above development is shown in Table 5.4-1. These safety functions will be confirmed during the fault studies performed as part of GDA.

Table 5.4-1: High level safety functions in UK ABWR

Fundamental Safety Function	No	High Level Safety Function
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	Functions to circulate reactor coolant
	1-6	Function of alternative reactivity control
2. Fuel Cooling	2-1	Functions to cool reactor core
	2-2	Functions to make up water for fuel storage pool
	2-3	Functions to retain reactor coolant (other than above)
	2-4	Functions to mitigate reactor pressure increase with other system
	2-5	Functions to suppress reactor power increase with other system
	2-6	Functions to make up reactor coolant with other system
	2-7	Function of alternative fuel cooling
3. Long term	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 (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)
	4-4	Functions to reseat safety valves and relief valves
	4-5	Functions to confine radioactive materials, shield radiation, and reduce radioactive release
	4-6	Functions to contain radioactive materials in the event of a severe accident
	4-7	Functions to prevent the dispersion of fission products into reactor coolant
	4-8	Functions to minimise the release of radioactive gases
	4-9	Functions to store the radioactive materials as gaseous waste
	4-10	Functions to store the radioactive materials as liquid wastes
5. Others	5-1	Functions to generate actuation signals for the engineered safety features and reactor shutdown system
	5-2	Supporting functions especially important to safety
	5-3	Functions to monitor plant conditions in case of an accident
	5-4	Functions to clean up reactor coolant
	5-5	Functions to shut down safely from outside the control room
	5-6	Functions to supply electric power (except for emergency supply)
	5-7	Functions for plant instrumentation and control (except for safety protection function)
	5-8	Auxiliary functions for plant operation
	5-9	Functions important to emergency measures and monitoring of abnormal conditions
	5-10	Function of alternative supporting system
	5-11	Functions to handle fuel safely

5.4.3 Categorisation of Safety Functions

For each event identified in the Fault Schedule, 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 (if possible) 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 depends on which is reasonably practicable. 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 offsite power).

Following HSE's Safety Assessment Principles, 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
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 and with initiating fault frequency > 10^{-5} /year, 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} /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.
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) accidents, 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.

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.

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.

All categorisations of safety functions will be confirmed during the fault studies presented in Chapter 24 and 26 of this PCSR.

5.4.4 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.

Again following HSE's Safety Assessment Principles, 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
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.

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.

Class 3 Other SSCs claimed as providing a second-line means of delivering a Category B safety function or as delivering a Category C safety functions.

SSCs in Class 1 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}/year), each identified safety function is required to have a diverse means of delivery. SSCs claimed to provide this diversity are classified as at least Class 2.
SSCs identified to provide Category B safety functions in Beyond Design Basis assessments or in the protection against Foreseeable Events are classified as Class 2.

Class 3 SSCs have safety importance but do not fulfill the requirements for Class 1 or Class 2. 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 will be categorised as category C and any SSCs identified to fulfill them will be classified as Class 3.

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 should, therefore, be classified as Class 2 or Class 3. For the UK ABWR, such SSCs are classified:

Class 2 if there is a single or redundant means of protection against their failure or maloperation.
Class 3 if there is diverse means of protection against their failure or maloperation.

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 that important system to fulfill its safety functions are considered to have the same class as the supported system.

- Supporting systems needed for that important system 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 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.

The above classification scheme is based on a fully deterministic approach. In the development of this PCSR, Probabilistic Safety Assessment (PSA) will be 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.

5.4.5 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 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 Codes and Standards section of this chapter of the PCSR.

(2) Examination, Maintenance, Inspection and Testing (EMIT) Requirements
In principle, all Class 1, Class 2 and Class 3 structures are the object of Examination, Maintenance, Inspection and Testing (EMIT). However, the specific requirements for EMIT (frequency, type, etc.) should be assigned according to the reliability claimed for each safety measure and the SSC's classification. This will be part of the engineering substantiation presented in the PCSR during GDA Step 4.

(3) Seismic Design
Seismic design of nuclear power plants provides mitigation in relation to radiological hazards by maintaining the integrity of SSCs during and after an earthquake. Therefore, each SSC is assigned to a seismic category that corresponds to radiological dose (off-site consequences) in case of the SSC failures due to an earthquake:

Seismic Category 1:	SSCs whose failure would lead to off-site dose > 10mSv and which must therefore maintain structural and functional integrity during and after Design Basis EARTHQUAKE (DBE) of 10^{-4} annual probability of exceedance earthquake.
Seismic Category 2:	SSCs whose failure would lead to off-site dose > 0.01mSv and which are therefore designed to maintain structural and functional integrity during and after 10^{-3} annual probability of exceedance earthquake.
Seismic Category 3:	SSCs whose failure would lead to off-site dose < 0.01mSv and which are designed by use of normal industrial standards for seismic design.

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

Seismic Category 1A:	SSCs whose failure could lead to the failure of an adjacent Seismic Category 1 SSC or which is required in Beyond Design Basis conditions. These SSCs must maintain their integrity during and after the DBE.

(4) Structural Design

There are some components, usually providing the containment safety function, 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.

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 would be considering the safety case for a steel Reactor Pressure Vessel (RPV). The RPV’s Major Boundary Portion like the 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 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 single or redundant protection against the failure of such Class 1 components, they may be classified as “High Integrity”. The safety case for these components does not require the same level of robustness.
If there is diverse protection against the failure of such Class 1 components, they may be 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 the Chapter 8 - Structural Integrity.

5.4.6 References

[Ref-1] Safety Assessment Principles for Nuclear Facilities, 2006 Edition Revision 1, Health and Safety Executive.

[Ref-2] Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions, IEC 61226:2009.

[Ref-3] Safety of Nuclear Power Plants: Design, Specific Safety requirements, IAEA, No. SSR-2/1, 2012.