Form10/00

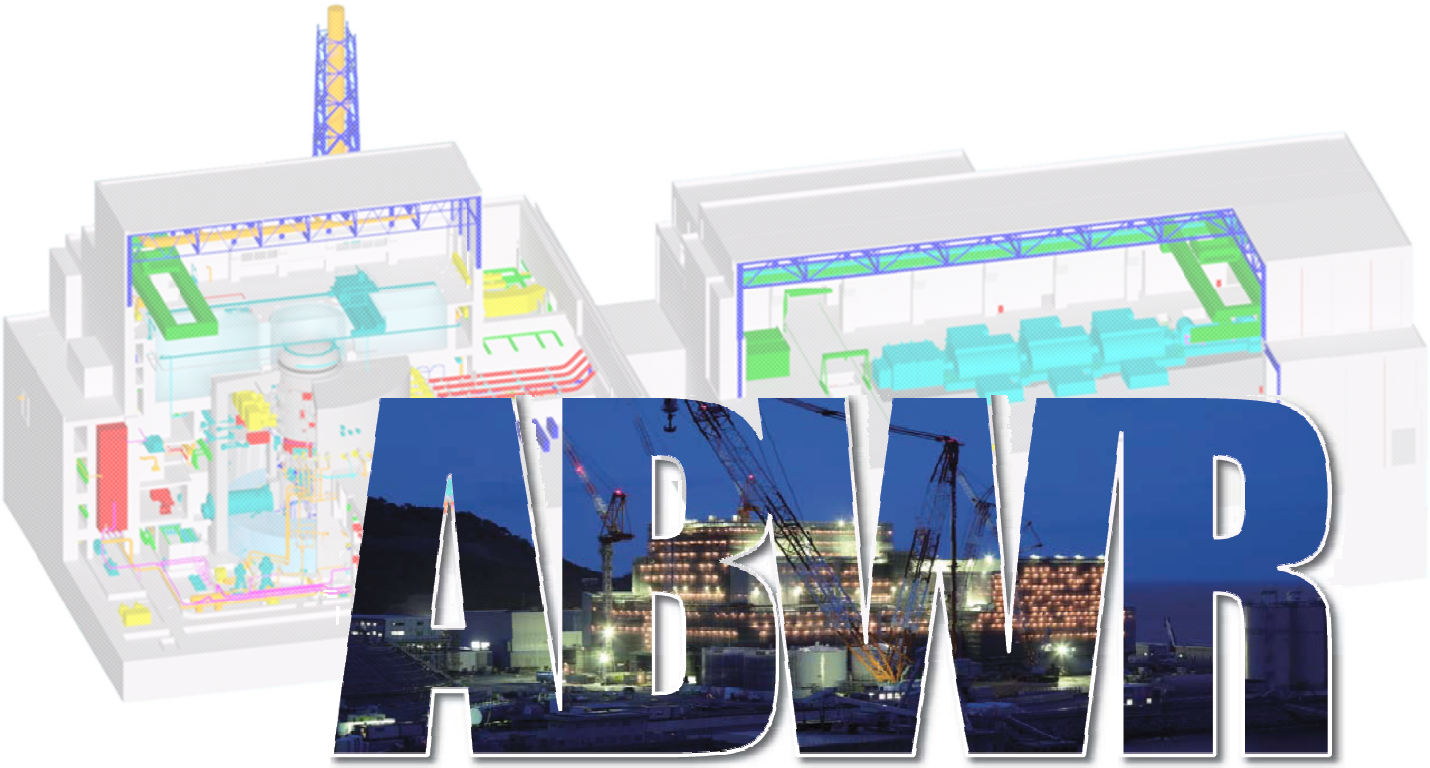
HITACHI

UK ABWR

Document ID	:	GA91-9101-0101-07000
Document Number	:	SE-GD-0127
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 7 : Internal Hazards



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

This Chapter demonstrates that the UK ABWR is tolerant to internal hazards. An internal hazard is any event originating within the boundary of a generic site that is capable of damaging the reactor or any of its supporting systems, and which could prevent safety systems from delivering the nuclear safety functions required of them. It lists the high level Safety Functional Claims related specifically to internal hazards.

UK and international good practice has been used to identify all relevant internal hazards (e.g. internal fire or flood, pipe whip, etc.) which have been listed and assessed in this Chapter.

At a high level, protection against internal hazards is provided by multiple redundant safety systems that are physically separated into three safety divisions by robust barriers. Generally, only equipment within one division is necessary to maintain safety, and if a hazard occurs in one division, the plant is designed so that safety systems in the other divisions can still perform their safety functions.

This Chapter systematically steps through each of the internal hazard groups, providing a summary of the detailed assessment work that underpins it. For each hazard group, the Chapter describes the design basis internal hazard assumed in the analysis, the protection provided by the design and the conclusions of the analysis. For all of the hazard groups, the analysis has shown that adequate protection is provided by the design.

There are some areas of the plant where it is not possible to rigorously separate safety systems between divisions. These areas include inside the Primary Containment Vessel and at the Main Control Room.

Reasonably foreseeable combinations of internal hazards have also been identified and assessed, including coincidental events (e.g. a flood occurring at the same time as a fire in another area), and consequential events where one hazard causes another (e.g. a dropped load damaging high energy pipework leading to further damage due to pipe whip). Internal hazards can also occur in combination with external hazards (e.g. a seismic event could lead to an on-site fire, explosion, or other internal hazard).

It is recognised in the Chapter that detailed analysis of some of these hazard combinations cannot be completed in GDA, but it is anticipated that an Internal Combined Hazards event will not affect SSCs required for safety and that redundant systems remain available to ensure the delivery of the Fundamental Safety Functions. Therefore, it is anticipated that the nuclear safety risks of the design will be demonstrated to be tolerable and As Low As Reasonably Practicable (ALARP) post-GDA.

This Chapter concludes that the risks due to internal hazards for the ABWR have been reduced ALARP. It is acknowledged that further work will be required post-GDA to develop the design and fully incorporate site specific aspects. This work will be the responsibility of any future licensee.

7.1 Introduction

7.1.1 Introduction

Pre-Construction Safety Report (PCSR) Chapter 7 demonstrates that the United Kingdom Advanced Boiling Water Reactor (UK ABWR) is tolerant to Internal Hazards, i.e. hazards that arise within the site boundary such as fires or flooding. Any event arising within any building on site or on the site itself that has the capability to damage the reactor or any of the supporting systems, or render any of them inoperable or of reduced capability is a potential Internal Hazard. This Chapter identifies such events, demonstrates that there is suitable diversity and redundancy of Structures, Systems and Components (SSCs) to ensure that Fundamental Safety Functions (FSFs) are met and that the residual risks from Internal Hazards are As Low As Reasonably Practicable (ALARP).

7.1.2 Background

An important part of the safety case is the demonstration that the reactor and support systems are fault tolerant. This means that the safety provisions provide, as a minimum, a withstand to all faults making up the Design Basis, such that dose targets on-site and off-site are met and risks are ALARP.

Faults may arise from failures of the reactor or supporting systems themselves, from failures of power generating systems or may arise from events outside those systems. Potential events outside the reactor, support systems and power generation systems are termed ‘hazards’ and fall into two main groups: those arising off-site and generally outside the control of the station operating organisation (External Hazards), and those arising on-site and generally within the control of the station operating organisation (Internal Hazards).

There is also the possibility that hazards may occur in combination, either coincidentally (for example a flood occurring in one location whilst a fire is occurring somewhere else) or by an Internal or External Hazard causing another hazard (for example a missile leading to a pipe rupture and flood). All such combinations are considered within this PCSR Chapter.

Faults and hazards are listed in the Fault Schedule (Table 4.2-1 of the Topic Report on Fault Assessment [Ref-17]) and Internal Hazard Schedules presented in each Level 2 Internal Hazards Topic Report (see Appendix C: Document Map) together with the safety provisions that make the reactor and support systems tolerant of those faults and hazards. This is discussed further in Sections 7.3.1.6 and 7.3.3.

For Internal Hazards, the primary means of protection are barriers which segregate normal operating systems and the redundant and/or diverse class 1 safety systems providing the same Fundamental Safety Functions. Much of the demonstration that the reactor is tolerant to Internal Hazards is provided by the demonstration barriers do not fail when subject to these hazards, this is supported by the use of separation and qualification of safety systems, where required, to withstand the hazard.

The main technical content of the Chapter summarises the contents of the individual Level 2 Topic Reports on the assessment of Internal Hazards as shown in the document map in Appendix C.

7.1.3 Document Structure

Following on from this introduction, Section 7.2 defines the Purpose and Scope of the Chapter. Section 7.2 also presents the individual Internal Hazards that have been determined as applicable to the UK ABWR. Section 7.3 describes how the Internal Hazards assessment fits into the overall safety case as well as describing the general philosophy of protection using barriers to prevent the failure of systems required to protect the reactor against the event or to prevent the loss of more than one Class 1 division. The way in which hazards can combine is discussed and summarised in Section 7.16.

The remainder of the Chapter then provides an assessment of the identified hazard groups. For each, there is an assessment of the Design Basis hazard and of the protection afforded by the plant design. In the case of Internal Hazards, this protection is mainly by engineered barriers between Class 1 divisions and between safety systems and normal operating systems; principally provided by reinforced concrete Class 1 divisional barriers that segregate the different trains of redundant safety equipment known as 'divisions'.

The Chapter is structured as follows:

Section 7.2	Purpose and Scope.
Section 7.3	General Principles – the general principles underlying the Internal Hazards assessment carried out are discussed here.
Section 7.4	Fires and explosions Internal Hazards assessment [Ref-2].
Section 7.5	Flooding, including water spray and steam release Internal Hazards assessment [Ref-3].
Section 7.6	Pipe whip and jet impact Internal Hazards assessment [Ref-4].
Section 7.7	Dropped and collapsed loads Internal Hazards assessment [Ref-5].
Section 7.8	Missiles Internal Hazards assessment [Ref-6].
Section 7.9	Blast (non-combustible effects e.g. blast following pressure part failure) Internal Hazards assessment [Ref-7].
Section 7.10	Electromagnetic Interference / Radio Frequency Interference (EMI/RFI) Internal Hazard assessment [Ref-8].
Section 7.11	Miscellaneous Internal Hazards assessment [Ref-9].
Section 7.12	Primary Containment Vessel (PCV) Internal Hazard assessment [Ref-10].
Section 7.13	Main Control Room (MCR) Internal Hazard assessment [Ref-11].
Section 7.14	Main Steam Tunnel Room (MSTR) [Ref-12].
Section 7.15	Turbine Disintegration [Ref-13].

Section 7.16	Combined Internal Hazards [Ref-14].
Section 7.17	Assumptions, Limits and Conditions for Operation (LCO) that relate to the Internal Hazards.
Section 7.18	Summary of the ALARP justification for Internal Hazards.
Section 7.19	Overall conclusions.

Individual Topic Reports provide detailed information on internal hazard assessment of each of the groups of hazards corresponding to the Chapter Sections above. These Topic Reports are themselves supported by lower level documents giving data for each room in the plant, substantiation of barriers and Topic Reports on specific issues such as doors on Class 1 barriers [Ref-16], the location of the Emergency Diesel Generators (EDGs) [Ref-24] and discussion of the Internal Hazards case for the Main Steam Tunnel Room [Ref-12].

The Chapter also has links to other PCSR Chapters, including the following;

- the consideration of Internal Hazards arising as a consequence of External Hazards is presented within PCSR Chapter 6: External Hazards,
- the context of assumptions, limits and conditions is presented within PCSR Chapter 4: Safety Management throughout Plant Lifecycle,
- Design Basis Analysis is presented within PCSR Chapter 24: Design Basis Analysis,
- Probabilistic Safety Assessment (PSA) including the PSA for hazards, is described in PCSR Chapter 25: Probabilistic Safety Assessment,
- General requirements related to conventional safety aspects are described in PCSR Chapter 4: Safety Management throughout Plant Lifecycle,
- NSEDP compliance is evaluated in the Topic Report on Compliance of UK ABWR Design with Nuclear Safety and Environmental Design Principles (NSEDPs - XE-GD-0743), and is summarised within PCSR Chapter 5 section 5.3,
- For generic links to GEP, and CSA documentation, please refer to Generic PCSR Chapter 1: Introduction. For GEP, where specific references are required, e.g. in Radioactive Waste Management, Radiation Protection, Decommissioning, these will be included in the specific sections within the relevant chapter.

7.2 Purpose and Scope

7.2.1 Purpose

The purpose of the Chapter is to demonstrate that UK ABWR is tolerant to Internal Hazards, hazards that arise within the plant, such as fires or flooding, and demonstrate that the residual risk from Internal Hazards is reduced to a level that is tolerable and ALARP. Any event arising in any building on site or on the site itself that has the capability to damage the reactor or any of the supporting systems, or renders any of them inoperable or of reduced capability is a potential Internal Hazard. The Chapter presents a summary of the analyses of the individual and combined hazards identified above.

Consistent with the Topic report on the Approach to Internal Hazards [Ref-1]; for each Internal Hazard:

- An assessment of how the Internal Hazard affects SSCs in the UK ABWR is performed,
- How loss of those SSCs might impact the ability to deliver the High Level Safety Functions/ Fundamental Safety Functions is determined, and
- Safety measures required such that there are always suitable and sufficient A-1 and/or A-2 SSCs remaining following any Internal Hazard to deliver the Fundamental Safety Functions are identified.

For most of the buildings and hazards, the demonstration of tolerance to Internal Hazards is based on claims relating to barriers as discussed in section 7.3.1 below. These postulated internal hazards impose design basis requirements on the civil structures of the UK ABWR as discussed in PCSR Section 10.3.3 of Chapter 10.

There are a small number of locations where it is not possible to claim barriers between Class 1 divisions: mainly the Reinforced Concrete Containment Vessel (RCCV), Main Steam Tunnel Room and parts of the Control Building. These locations are the subject of specific Topic Reports where the corresponding High Level Safety Functional Claims relating to segregation and other forms of protection are discussed.

7.2.2 Scope of Assessment

A complete list of Internal Hazards has been derived by reference to open literature sources, Regulator guidance, experience from previous UK nuclear plant Internal Hazard assessments and engineering judgment. The compiled list is based on the potential hazard effects and whether it is bounded by another hazard that has already been identified (see [Ref-15]). It is shown that assessment of these Internal Hazards is sufficient to bound all credible Internal Hazard effects. This is in line with relevant modern UK and international good practice.

The hazards identified are examined to determine whether they can be screened out on the following basis:

- Inspection – the hazard is not relevant to this plant or cannot occur on this site.
- Effect – the impact of the hazard has an insignificant effect.
- Frequency of occurrence – the frequency of the hazard that could cause damage is small in comparison with the frequency of hazards that result in a large uncontrolled release [Ref-32].
- Bounded hazard – the failures induced by the hazard are bounded by another hazard of similar effect and higher frequency.

Where the hazard could not be screened out it is included in the design basis assessment [Ref-15].

The following hazards (individually and in combination) are covered in detail in the sections below:

- Internal fire and internally initiated Explosions.
- Internal flooding.
  - Immersion.
  - Spray.
  - Steam Release.
- Pipe whip and liquid jet impact.
- Dropped loads and collapsed loads.
- Internally generated missiles.
  - Conventional missiles.
  - Turbine Disintegration.
- Blast effects (non-combustible effects e.g. blast following pressure part failure).
- Internally generated Electromagnetic Interference (EMI) and internally generated Radio Frequency Interference (RFI).

There are also a number of less significant hazards that are dealt with in Section 7.11 (Miscellaneous Internal Hazards). These are:

- On-site hazardous materials.
- On-site transportation accidents.
- Pipeline accidents.
- Natural gases from the ground e.g. methane.

Excluded are any hazards that arise outside the site boundary and outside the control of the station operating organisation.

The scope of the buildings included in the GDA design is given in PSCR Chapter 10, Section 10.2.2. The assessment of the resilience of buildings to Internal Hazards has focused on those buildings from which a hazard originates, or contain systems important to safety within them:

- Reactor Building (R/B) (including PCV, which has its own Topic Report).
- Control Building (C/B) (including Main Control Room (MCR) and Main Steam Tunnel Room (MSTR), which have their own Topic Reports).
- Heat Exchanger building (Hx/B).
- Filter Vent Building (FV/B).

- Emergency Diesel Generator Buildings (EDG/B).
- Back-up Building (B/B).
- Turbine Building (T/B).
- Radwaste Building (Rw/B).
- Service Building (S/B).
- GDA relevant service tunnels (S/T).
- Yard, including separate tanks e.g. Condensate Storage Tank (CST), Light Oil Tank (LOT), and FLSS Water Storage Tanks.

Excluded are any buildings which contain hazard sources that do not challenge the delivery of the Fundamrntal Safety Functions or are outside the GDA scope such as the Administration building.

The assessment includes all operating phases of the reactor (construction phases are excluded as there is no radiological hazard at this time):

- Power operation.
- Startup.
- Hot shutdown.
- Cold shutdown.
- Refuelling outage.

It should be noted that this PCSR Chapter does not consider the environmental and security aspects of the UK ABWR design. For links to the Generic Environmental Permit and Conceptual Security Arrangements please refer to PCSR Chapter 1: Introduction.

7.3 General Principles

7.3.1 General Principles for Protection against Internal Hazards

Hazards protection is achieved mainly by prevention, limitation of severity and mitigation which is provided by segregation/separation of redundant and diverse equipment or by qualification. In some cases a combination of approaches is used.

7.3.1.1 Approach to Delivery of Fundamental Safety Functions

With respect to hazards protection, the design of the UK ABWR is primarily based on providing redundant, diverse and segregated safety systems. The safety systems for the UK ABWR can be divided into two main groups:

- the systems that prevent faults and abnormal conditions in the facilities, and
- the systems that mitigate the consequences of a fault and abnormal events.

These safety systems are required to ensure that the following FSFs are still delivered when a fault occurs:

- **FSF1: Control of reactivity** and ability to achieve emergency reactor shutdown;
- **FSF2: Fuel cooling** to prevent fuel damage;
- **FSF3: Long term heat removal**, including removal of decay heat and containment venting systems;
- **FSF4: Confinement/Containment of radioactive materials**;
- **FSF5: Others**, including support to safety systems, fuel handling, remote shutdown capabilities, instrumentation and monitoring, alternative power supplies and emergency measures.

The implementation of this safety philosophy is based upon redundant, diverse and segregated safety systems that deliver the FSFs addressed in PCSR Chapter 5, Section 5.6.2 “ABWR Safety Functions”. Each FSF is further broken down into High Level Safety Functions (HLSFs). For the purposes of the Internal Hazards assessment HLSF 5-7 “Functions to limit the effects of hazard” is the key HLSF.

7.3.1.2 Classification of Safety Systems to Maintain Fundamental Safety Functions

Three mechanical and four control and instrumentation (C&I) divisions are provided for the principal cooling and support systems and redundant, segregated and diverse SSCs are available to deliver all FSFs. As described in Section 5.6 ‘Categorisation and Classification of Structures, Systems and Components (SSCs)’ of PCSR Chapter 5, the primary means of delivering the Category A functions are classified as Class 1 systems. In addition to these Class 1 systems, secondary means of delivering the Category A functions are also identified and these are classified as Class 2 systems.

Table 7.3-1 below shows the redundancy and diversity of the safety systems that are claimed within the safety case as key to maintaining the Fundamental Safety Functions. This is a subset of the safety systems available in the UK ABWR design. The system descriptions can be found in the respective Sections of PCSR Chapters 12, 13 and 19 as shown below.

Table 7.3-1: Summary of Safety Systems

Function		System	Redundancy / Segregation
Reactivity control and reactor shutdown		Control Rod Drive (CRD) [Chapter12, Section 12.4.3.1 in PCSR]	Hydraulic Control Units are distributed in two rooms, both are required for reactor shutdown [Chapter12,Section 12.4.3.1 in PCSR]
		Standby Liquid Control System (SLC) [Chapter12, Section 12.4.3.2 in PCSR]	High pressure positive displacement pumps to inject boron for diverse shutdown [Chapter12, Section 12.4.3.2 in PCSR]
Cooling	Core	Division I: Reactor Core Isolation Cooling System (RCIC)+[Automatic Depressurisation System (ADS) + Low Pressure Flooder (LPFL)(A)] Division II: High Pressure Core Flooder System (HPCF)(B) + (ADS+LPFL(B)) Division III: HPCF(C)+ (ADS+LPFL(C)) [Chapter13, Section 13.4.1 in PCSR]	2 Segregated trains of HPCF (electrically driven) [Chapter13, Section 13.4.1 in PCSR]
			1 Segregated train of RCIC (steam driven) [Chapter13, Section 13.4.1 in PCSR]
			3 Segregated trains of LPFL (electrically driven) [Chapter13, Section 13.4.1 in PCSR]
	Spent fuel	Fuel Pool Cooling and Cleanup System (FPC) [Chapter19, Section 19.9 in PCSR]	2 Segregated trains of FPC (pumps and heat exchangers) 2 Segregated trains of Residual Heat Removal System (RHR) in fuel pool cooling mode (pumps and heat exchangers) [Chapter19, Section 19.9 in PCSR]

Function	System	Redundancy / Segregation
Containment	PCV [Chapter13, Section 13.3.3.1 in PCSR]	RHR in Suppression Pool (S/P) cooling mode [Chapter13, Section 13.3.3.4 in PCSR] RHR in containment vessel cooling spray mode [Chapter13, Section 13.3.3.4 in PCSR] Containment isolation (by valves located inboard and outboard to the PCV) [Chapter13, Section 13.3.3.2 in PCSR]
	Secondary Containment (R/B) [Chapter13, Section 13.3.4.1 in PCSR]	Standby Gas Treatment System (SGTS) [Chapter13, Section 13.3.3.3 in PCSR]

Two diverse systems, Control Rod Drive System (CRD) and Standby Liquid Control System (SLC) deliver reactivity control and reactor shutdown function. The CRD system also has two diverse methods to drive control rods into the core (hydraulic backed up by electrical motor). To protect the function against consequences of Internal Hazards, the UK ABWR is designed to provide physical segregation between the CRD and SLC systems so as to protect at least one system from the hazard. In addition, the hydraulic function of the CRD system is designed as fail-safe so in the event of a failure due to Internal Hazard, a SCRAM is automatically initiated (see PCSR Chapter 12: Reactor Coolant Systems, Reactivity Control Systems and Associated Systems, Section 12.4.3.1 for more details).

Cooling of the fuel in the core and spent fuel in the Spent Fuel Storage Pool (SFP) is required. For core cooling there are three redundant safety trains in three segregated divisions. Each of the divisions provides high pressure core injection, Reactor Pressure Vessel (RPV) depressurisation and low pressure core injection to cool the core fuel. The UK ABWR design ensures delivery of the core cooling function by robust Class 1 divisional barriers between the divisions so as to prevent hazards spreading beyond a single division (see PCSR Chapter 13: Engineered Safety Features, Section 13.4.1 for more details).

The spent fuel cooling function is delivered by the FPC backed up by two redundant RHR pumps in SFP cooling mode. As noted above, each of these trains is segregated by divisional barriers. Spent fuel remains in the SFP until it is cool enough for transfer to long term storage which utilises passive cooling within specially designed fuel storage casks (see PCSR Chapter 19: Fuel Storage and Handling, Section 19.9 for more details).

The containment cooling function is delivered by the RHR in S/P cooling mode as the primary means of heat removal. Other means of containment cooling is provided by the PCV spray cooling mode of the RHR. The containment of PCV is ensured by inboard and outboard containment isolation for each of the penetrations. There is no redundant primary containment, however an additional containment function is delivered by secondary containment, which is supported by two divisions of the SGTS.

The safety systems summarised in Table 7.3-1 are supplemented by an independent set of nuclear safety mitigation equipment (typically Class 2) that can be used for core cooling, decay heat removal and maintaining primary containment. These are located in seismically qualified buildings (Backup Building (B/B) and Filter Vent Building (FV/B))

7.3.1.3 Classification of Safety Systems to Maintain Separation and Segregation of Divisions

The Class 1 mechanical and C&I divisions described above are segregated by robust barriers (divisional barriers) which contain an Internal Hazard within the affected division and prevent the spread of the hazard to a different division. These divisional barriers provide the principal means of maintaining the Fundamental Safety Functions against the effect of Internal Hazards and in accordance with Section 5.6 'Categorisation and Classification of Structures, Systems and Components (SSCs)' of PCSR Chapter 5, the divisional barriers are generally classified as Class 1 structures and are designed to Nuclear Safety Class 1 standards. The Internal Hazards Barrier Substantiation Report [Ref-34] demonstrates that the divisional barriers meet their required safety functions for all Internal Hazards.

In addition to the claims made on the Class 1 divisional barriers, a number of additional SSCs are claimed on a hazard by hazard basis (for example, floor gratings are claimed as part of the engineered flood paths and blow out panels are claimed as part of the engineered steam release paths). Where claimed, these additional SSCs are discussed in the hazard specific summaries (in Sections 7.4 to 7.16).

7.3.1.4 Safety Claims and Arguments

In order to demonstrate that the HLSF discussed in section 7.3.1.1, the HLSF is articulated in the form of a Safety Function Claim (SFC). These claims are supported by arguments and evidence that collectively demonstrate that the HLSF is achieved.

The claims are in **bold**, and arguments follow in *italics*.

7.3.1.5 General Safety Claims

The following Internal Hazards Safety Claim is the top-level safety claim that applies to all Internal Hazards. As the Fundamental Safety Functions can generally be delivered from any one division on its own, the hazard-specific safety claims need only relate to preventing any given Internal Hazard

event from affecting safety-related equipment outside its division of origin. Appendix A presents the full claims table for this PCSR Chapter.

General Claim IH_SFC_5-7.1: Internal Hazards do not prevent the delivery of the Fundamental Safety Functions.

The overall Internal Hazard Safety Case demonstrates that no individual or combined Internal Hazards will prevent the delivery of the FSFs. This is fulfilled by the provision of suitable segregation to prevent the extension of an Internal Hazard outside the compartment where it is originated, the separation of equipment within the same compartment to prevent hazard propagation, or the qualification of SSCs to withstand the hazard. The combination of segregation, separation and qualification will ensure that sufficient equipment is available to fulfil the FSFs during and after the hazard event.

General Claim IH_SFC_5-7.2: The consequences of any Internal Hazard are limited to one division, except for areas covered by General Claim IH_SFC_5-7.3.

The UK ABWR design is such that General Claim IH SFC 5-7 is chiefly delivered by the provision of physically segregated divisions of safety-related equipment providing the same function. It is demonstrated that all design basis Internal Hazards (independent, combined or correlated) will have consequences limited to one division.

General Claim IH_SFC_5-7.3: Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after an Internal Hazard, to fulfil the Fundamental Safety Functions.

Although the general argument is that safety-related equipment from the same division is segregated by Class 1 barriers, there are some exceptions to this arrangement. Where this is the case, either sufficient A-1 or A-2 SSCs are qualified to deliver the Fundamental Safety Functions under the conditions of the Internal Hazard event, or the SSCs are protected in some way from the consequences of the event such that delivery of their Fundamental Safety Functions is not prevented.

The general claim for exceptions to segregation will apply to all Internal Hazards. The arguments and evidence for this claim related to the PCV, MCR and MSTR are found in [Ref-10], [Ref-11], and [Ref-12] respectively.

The overall objective is thus to ensure that at least one division of equipment is available to maintain the Fundamental Safety Functions.

Where required by the hazard assessment, these general claims are supported by hazard specific claims which together demonstrate that these general claims have been achieved. This provides an auditable and logical process for demonstrating that the design intent has been achieved.

7.3.1.6 Relationship between Internal Hazards and the Fault Schedule (Bounding Fault).

Comprehensive Hazard Schedules, containing all bounding hazard events, are presented within the Topic Reports on Internal Hazards. All bounding hazard events are linked to bounding faults, as identified in the Fault Schedule (Table 4.2-1 of the Topic Report on Fault Assessment [Ref-17]) and discussed in PCSR Chapter 24: Design Basis Analysis.

The bounding fault identified for most Internal Hazard events is a Loss of Offsite Power (LOOP) event concurrent with any single Internal Hazard event. The LOOP event bounds loss of some non-safety related equipment caused by the Internal Hazard. All non-safety related power supplies and equipment could be disabled during a LOOP event. Therefore, an Internal Hazard event concurrent with a LOOP event would result in the most limiting available equipment to fulfil the Fundamental Safety Functions, i.e. all non-safety related equipment and one division of safety related equipment is unavailable.

The Fault Schedule indicates that the Internal Hazard effects must be limited to one division (Claim IH_SFC_5-7.2) except where otherwise justified (Claim IH_SFC_5-7.3 and section 7.3.1.9) for all faults to enable delivery of the Fundamental Safety Functions.

7.3.1.7 Prevention and Limitation of Severity of Internal Hazards

Prevention of Internal Hazards starts with the design processes and procedures. These processes lead to limiting the sources of potential hazards. Whenever possible, design guides, and codes and standards are used to appropriately design equipment and structures. This assists in developing a layout to prevent the occurrence of an Internal Hazard which therefore prevents the impact of Internal Hazards. The details of prevention measures are given in each Internal Hazard section.

The specific Internal Hazard assessments identify and assess the prevention measures included in the design. Classifications of these measures are determined on the importance of the prevention measure in delivering the Fundamental Safety Functions and reducing risk to ALARP. As stated earlier, significant importance and a higher classification are placed on mitigative measures and most of the preventative measures are classified as defence in depth.

Some Internal Hazards have measures to limit the severity of the hazards in order to reduce the consequences or risk of the hazards (e.g. firefighting). The details of the measures are also described in the Internal Hazard sections.

7.3.1.8 Mitigation of Internal Hazards

If all the prevention measures were to fail, an Internal Hazard will not prevent delivery of the FSFs so long as its effects can be contained to systems belonging to no more than one division of primary (A-1) safety systems. In some areas, it is necessary to consider an Internal Hazard initiating a secondary Internal Hazard. These combined Internal Hazard events have been assessed in the section below and, where required, additional prevention and mitigation measures are identified. Internal Hazards claims are achieved with the following design features:

- SSCs delivering Fundamental Safety Functions which require redundancy are located in segregated Class 1 divisions fully enclosed with appropriately designed Class 1 divisional or non-divisional barriers (floor, ceiling, wall, etc.). Class 1 divisional barriers are designed to withstand the potential consequences of the various identified Internal Hazards.
- Penetrations in Class 1 divisional barriers are minimised. Any penetrations in a Class 1 divisional barrier such as doors, ductwork, hatches, pipework and cables are appropriately designed and sealed with the same hazard resistance as the barrier, where possible.
- Where sufficient provision of divisional segregation (as described above) is not possible, then additional measures are considered, which may include the following:
    - Administrative controls on the amount of materials that may cause an Internal Hazard;
    - Separation by individual room walls or equipment barriers (non-divisional barriers);
    - Separation of equipment by distance, without intervening materials that may cause spread of, or additional Internal Hazard;
    - Local passive protection that may prevent Internal Hazards affecting the equipment required to function.

Where door access through a claimed Class 1 divisional barrier is required, two sets of doors separated by a lobby are provided wherever reasonably practicable. Any remaining single doors are fitted with an alarm system to alert operational staff where doors are left open or fail to close. This issue was discussed during Steps 3 and 4, and the issue is described in Topic Report of Doors Class 1 Barriers [Ref-16].

7.3.1.9 Exceptions to Divisional Segregation

The UK ABWR design implements the nuclear safety principles of redundancy, diversity and segregation in order to reduce risks ALARP. However, in some instances strict adherence to these principles may not result in a reduction in risks. In particular, where there are A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment; this arrangement can still be an ALARP solution and justifiable. Such A-1 or A-2 SSCs are referred to as exception to segregation SSCs. The most significant exceptions are the PCV, MCR and MSTR and these have been demonstrated to be acceptable in their own detailed assessments as summarised in Sections 7.12, 7.13 and 7.14 respectively, other exceptions to segregation SSCs are discussed in each hazard specific Section below.

For areas outside of PCV, MCR or MSTR, the Topic Report on Exceptions to Segregation [Ref-25] has demonstrated on a case-by-case basis how the FSFs can still be delivered following an Internal Hazard that affects such exceptions to segregation SSCs.

7.3.2 Internal Hazards Assessment

7.3.2.1 Internal Hazards Assessment Method

The approach for demonstrating tolerance to Internal Hazards is composed of five steps:

(1) Identifying the classes of hazards that should be considered as Internal Hazards for the UK ABWR.
(2) Identifying the sources of Internal Hazards in the design and where possible eliminating or reducing the hazard.
(3) Identifying the Internal Hazards within the design basis based on their frequency of occurrence.
(4) Identifying faults that may occur due to the hazard and the mitigative systems that are required to deliver safety functions.
(5) Evaluating the effects of Internal Hazards and ensuring that sufficient equipment is available to deliver the Fundamental Safety Functions.

Each individual Internal Hazard assessment includes additional steps for assessing the specific hazards as presented in Sections 7.4 to 7.16.

7.3.2.2 Combinations of Internal Hazards

Combined as well as single Internal Hazards are considered as part of the comprehensive Internal Hazards assessment. There are three distinct mechanisms in which design basis Internal Hazards may occur in combination. These are:

- **Consequential Hazards;** Consequential hazards are defined as an event causing a primary hazard that may give rise to one or more consequential, secondary hazards due to a direct causal relationship between the primary and secondary hazard.
- **Correlated Hazards;** A single internal correlated event is identified and as a result multiple simultaneous hazards are initiated as a consequence from this single initial event. The underlying cause could be either internal or external.
- **Independent Hazards;** Internal Hazards are considered to be independent if they could only be expected to occur together by random coincidence, due to there being no causal association between the initial events. The simultaneous occurrence of hazards also includes hazards that occur in succession of another fault or hazard, which may have resulted in safety related plant being degraded or compromised.

Generally, only a single independent Internal Hazard is postulated to occur at any given time as most hazards are infrequent, and the frequency of two infrequent and independent events occurring simultaneously or within a short time period is extremely low. Therefore, it is possible in many instances to exclude independent Internal Hazards, where they are not consequentially linked on a frequency basis.

7.3.2.3 Combinations of Internal and External Hazards

An external hazard could cause an Internal Hazard, for example a seismic event could cause a flood due to failure of non-seismically qualified pipework.

Non-causally related combinations of internal and external hazards are very low frequency events and are judged to be outside of the design basis for Internal Hazards.

7.3.2.4 Combinations of Internal Hazards and Single Failure

A single failure is a failure that results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it. For the purposes of Internal Hazard assessment, single failure is assumed to occur within a division other than division where the Internal Hazard originates. For Internal Hazards delivery of Fundermental Safety Functions will be still met under single failure assumption by the provision of segregated safety divisions of safety related Systems, Structures and Components (SSCs). [Ref-1].

7.3.2.5 Operator Response

In general, the Safety Case for Internal Hazards does not require short term operator intervention. If this is required no operator action within 30 minutes of the event has been claimed. Any claims which are required to be made on operator actions as a result of the Internal Hazards safety case are assessed within the Human Factors topic area and presented in PCSR Chapter 27: Human Factors.

7.3.2.6 Internal Hazards during the Shutdown Period

Internal Hazards that can occur during shutdown periods (including refuelling) are assessed in the same way as Internal Hazards during operation periods. The Internal Hazards and initiating faults to be considered may be different, as may be the safety systems to mitigate the hazards. This is because some systems will not be operating or cannot be in operation due to maintenance activities, in addition there are changes to compartmentation during the outage due to opening of hatches to facilitate large equipment movements. However, during shutdown, the risk is significantly reduced because the reactor will already be shut down. The cooling load is reduced and the reactor control rods are inserted.

The assessments of Fire and Explosion and Flooding Internal Hazards presented in Sections 7.4 and 7.5 below include a specific discussion on the Internal Hazards during these shutdown periods and the additional measures that are implemented to manage the hazards. These additional measures ensure that the FSFs continue to be provided during the shutdown period.

7.3.3 Consideration of Internal Hazards in the Fault Assessment

The Topic Report on Fault Assessment [Ref-17] utilises deterministic and probabilistic analysis to evaluate and assess the robustness of the plant. This is complimented by the Hazard Schedules that are addressed in each individual Level 2 Topic Report (Appendix C: Document Map). Contributions from Internal Hazards to initiating events through consequential failures of components or by

spurious actuation are identified as part of the development of the Fault Schedule and Hazard Schedules.

The Internal Hazards assessment largely takes the form of a compartment-by-compartment analysis to identify the effects of Internal Hazards and the potential for these hazards to be initiating events in the Fault Schedule. It considers important SSCs and how those SSCs are protected so the equipment and protection elements can be appropriately claimed to prevent and mitigate the Internal Hazard.

During the UK ABWR GDA, the Fault Schedule was updated in line with the Internal Hazards Safety Case to maintain consistency between the areas.

7.4 Internal Fire and Explosion

7.4.1 Introduction

The Topic Report on Fire and Explosion [Ref-2] considers the internal fires and explosions that can occur within the UK ABWR site boundary and buildings. Sources of combustible inventory include fuel oil, lubrication oil, cables and transient combustibles. Potential explosion hazards include oil mists, High Energy Arcing Faults (HEAF), hydrogen and other flammable gases. Fires and explosions may also arise from other internal and external hazards.

A comprehensive Hazard Schedule, containing all bounding fire and explosions hazard events identified, is presented within [Ref-2]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.4.2 Claims and Arguments

As for all other Internal Hazards, a principal objective of the internal fire and explosion safety case is to limit the effects of any fire or explosion hazard to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5. Appendix A presents the full claims table for this PCSR Chapter; no hazard specific claims are required for fire and explosion, however the following hazard specific arguments have been developed in support of claims IH_SFC_5-7.2 and IH_SFC_5-7.3:

(IH FE SFC 5-7.2.A1)
For category A functions which have multiple redundant divisions of Class 1 equipment, the divisions are segregated by Class 1 divisional barriers which function as 3 hour fire compartment barriers. The approach to barrier substantiation is presented within Section 4 of the Barrier Substantiation Report [Ref-34].

For the purpose of internal fire and explosion, the functional intent of divisional barriers is to protect against the consequence of a hazard event, such that the consequences will not undermine the function of Class 1 SSCs in any neighbouring division. This is achieved in general by limiting the event to the division in which the fire or explosion event originates. The loss of one such division of equipment is generally considered to be acceptable. Acceptability of such events, is demonstrated in the Hazard Schedules presented in Appendices A to K of [Ref-2].

(IH FE SFC 5-7.2.A2)
The combustible inventory in each room within a division is determined within [Ref-2] and it is demonstrated that design basis fires will be accommodated by the 3 hour fire resistant divisional barriers. Section 7.4.3.5 below describes the fire and explosion prevention measures in place that minimise both the use of flammable and explosive substances, and potential ignition sources.

(IH FE SFC 5-7.2.A3)

Penetrations in divisional barriers are minimised as far as is reasonably practicable and designed such that the overall Category and Class of the barrier (A-1) is maintained. This is achieved through the use of appropriate penetration seals, fire dampers within the HVAC system and 3 hour fire rated doors. This fire containment approach is discussed further in Section 7.4.3.11 below.

(IH FE SFC 5-7.3.A1 and IH FE SFC 5-7.3.A2)
Within any GDA building where hatches in the divisional barriers may be temporarily open during outages, a fire or explosion at this time will leave, as a minimum, one division of A-1 and one division of A-2 systems available to maintain the FSFs.

Exception to Segregation SSCs vulnerable to failure from fire or explosion are, where possible, designed to fail safe. In addition, alternative means of delivering the FSFs exist for all exception to segregation SSCs. As demonstrated in [Ref-25], these alternative means of delivering the FSFs are not vulnerable to the original fire or explosion hazard.

7.4.3 Design Basis

7.4.3.1 Fire and Explosion Hazard Analysis Methodology

The Fire and Explosion Hazard Analysis (FHA) has been performed based on the following approach:

(1) Identification of nuclear safety plant and equipment SSCs providing Fundamental Safety Functions that may be affected by an internal fire or explosion.
(2) Identification and evaluation of the fire and explosion hazards present in each room or area. This includes fire loadings and the potential for explosion overpressure.
(3) Characterisation of the fire and explosion hazard on nuclear safety plant and equipment in the affected room or area, which will generally be stated as the loss of function.
(4) Identification of the fire and explosion prevention and protection arrangements within each room or area, including fire resistant barriers, fire detection and fire suppression systems, and explosion mitigation.

This methodology is consistent with Section 7.2.1, including the further detail presented in section 7.3.2, and is designed to demonstrate how suitable and sufficient A-1 and A-2 SSCs will remain available to deliver the FSFs following any internal fire or explosion hazard in the UK ABWR. The detailed list of affected systems is presented in the Hazard Schedules for fire and explosion hazards presented in Appendices A to K of [Ref-2].

7.4.3.2 Assessment Assumptions

The following assumptions provide the basis for assessing postulated fire and explosion hazards during power operation:

- It is assumed that a fire can start at any times and at any location which contains permanent or transient combustible materials.

- When a fire or explosion event occurs in a fire separation division, it is conservatively assumed that all functions are lost for equipment, including electrical cables, within the same Class 1 division. It should be noted that this assumption is highly conservative and does not represent a real fire event in the UK ABWR.
- Only a single fire takes place at a given time, but this has the potential to spread to other areas.
- All combustible inventories within a given fire separation division are assumed to take part simultaneously in the event of a fire.
- Fire resistant characteristics of the 3-hour fire rated barriers are assumed to be same on both sides of the barrier (walls and ceiling/floor).
- The initiating event frequency of a fire event during power operations is conservatively assumed to be frequent (> 10^{-3} pa).
- The highest probable calorific value is used to calculate combustible load where detailed equipment specification was not available.
- The fire may occur as the result of local ignition or another internal or external event. All equipment, including cables, can be sources of ignition.
- Except where a particular local fire risk is identified, local fires lead to lower heat fluxes and temperatures than fires involving whole fire separation divisions. Therefore, local fire challenges to fire barriers are generally bounded by those from separation division fires.
- Hot shorts and spurious operation are addressed as part of the probabilistic safety assessment (PSA).

During outages when maintenance operations are in place, hatches may be opened to facilitate access of personnel and equipment, therefore challenging divisional segregation. The following assumptions are made for the outage assessment:

- During outages it is assumed that the requirements for the FSFs are less onerous due to the control rods being fully inserted and the decay heat is less than at power modes. The relevant FSFs are therefore long term cooling (FSF3), containment (FSF4) and Others (FSF5).
- Where equipment is moved through divisional Class 1 barriers, the doors will be opened only temporarily and will be closed immediately after passage.
- Hatches may be left open for one to two days. Therefore, it is assumed that fire separation divisions are connected where this occurs. Where there is any compromising of Class 1 barriers a temporary ‘fire watch’ will be provided during the time the barrier is breached.
- Temporary services are not run through doors during normal outage operations. This will only be done during plant modifications therefore it is not considered that these doors may be open as part of GDA.
- For all hazard scenarios that require initiation of Flooder System of Specific Safety Facility (FLSS), it is assumed that the FLSS is manually initiated to deliver the FSFs during outage (see PCSR Chapter 27: Human Factors, for further details of this Human Based Safety Claim.).

During the site specific stage, once the detailed outage schedule is available, the deterministic assessment for fire and explosion hazards during outages can be revised as necessary by the future licensee.

7.4.3.3 Design Requirement

With respect to fire and explosions, the internal hazard claims in Section 7.4.2 will be achieved in the UK ABWR by:

- **Minimising fire loading and explosion sources**, e.g. where practicable, use of non-combustible materials or storing explosive materials outside buildings important to safety.
- **Limiting the potential ignition sources**, e.g. designing electrical equipment to appropriate standards and guidance.
- **Limiting the severity of fires that do start** by e.g. early detection and automatic or manual suppression of fires.
- **Mitigating the consequences of fires and explosions** by relying on robust, reinforced concrete barriers that segregate the redundant, primary safety systems (A-1 SSCs) from each other and from the backup safety systems (A-2 SSCs).

7.4.3.4 Sources of Internal Fire and Explosion Hazards

The principal fire sources identified within the UK ABWR buildings and site are:

- **Power, control and instrumentation cables**, although cable design standards limit the risk of ignition and flame spread.
- **Electrical equipment**, e.g. control panels and motor control centres inside buildings and transformers in the Yard;
- **Combustible liquids*,** e.g. pump lubrication oils inside UK ABWR safety-related buildings and diesel/light oil stored in specially-designed buildings located in the Yard;
- **Flammable gases**, e.g. hydrogen or methane.
- **Transient combustible materials**, e.g. packaging materials or cleaning fluids.

*Note: the use of *flammable* liquids, i.e. those that are readily ignitable and have a low 'flashpoint', is very limited within buildings containing radiological material or safety systems that support the FSFs.

In addition, the following have been identified as explosion sources in the UK ABWR:

- **Hydrogen gas**, where used as part of the process or radiolytic* gases generated within process and plant;
- **Pressurised oils**, where they have the potential to produce flammable oil mists;
- **Medium/high voltage equipment**, where they have failure modes that could lead to High Energy Arcing Faults (HEAF).

* Hydrogen and oxygen is produced within the reactor core and some other supporting systems. Measures have been taken to reduce the generation of radiolytic gases and prevent their accumulation within process and plant (See Section 7.4.3.5 Fire and Explosion Prevention for more details).

7.4.3.5 Fire and Explosion Prevention

As discussed in Section 7.4.2, the UK ABWR is designed to minimise the use of flammable and explosive substances, as well as potential ignition sources (underpinning internal hazard Claim IH_SFC_5.7-2).

The likelihood for fires occurring is limited by the following design features:

- Non-combustible materials or fire retardant materials are used where practicable.
- Pipework containing flammable liquids is welded and sealed, and double walled where necessary.
- Equipment containing flammable liquids is pressure tested.
- Any leakage is detected by liquid level monitoring and captured.
- The area around equipment containing large quantities of combustible liquids includes bunds that prevent spread of the spill. These bunds are designed to contain additional liquid from any firefighting water/foam.
- Low combustibility fluids are used where practicable.
- Electrical equipment and cabling is designed to the design codes relevant for the intended use and environment, including those codes and guidance covering reliability, ignitability and fire resistance.
- Cables specified for the UK-ABWR meet appropriate standards for flame spread and smoke generation under fire conditions.
- Cables are installed in steel cable trays, conduits or other non-combustible cable supports and are appropriately spaced.
- Insulating lagging is provided for pipework with hot surfaces.
- Administrative controls will be established to limit combustible materials in certain areas, control the locations where combustible materials may be, and describe work processes that prevent ignition sources.
- The Emergency Diesel Generators (EDGs) are recognised as a potentially large fire source. For this reason and others, the EDGs are segregated both from each other (there are three redundant EDGs each capable of supplying all the plant's Emergency power) and from other primary and backup safety systems (A-1 and A-2 SSCs) by locating each EDG in its own dedicated building physically separated from the main UK ABWR buildings.

In addition, UK ABWR includes the following features designed to minimise explosion risk:

- Pipework for systems which contain hydrogen is designed to prevent leakage and failure. It includes welded joints, leak tight valves and complies with ASME Section III and B31.1

standards, in addition to meeting the UK Pressure Equipment Directive (PED), Pressure Systems Safety Regulations (PSSR) and other appropriate UK regulation.

- Pipework systems that may contain hydrogen due to the decomposition of water have been designed in accordance with ASME Sections III, VIII and B31.1 standards, in addition to meeting the Japanese design guide JANTI-NCG-01 for this specific hazard.
- A full assessment of the risk of radiolytic gases for the UK ABWR process and plant has been carried out on a pipe-by-pipe basis. Wherever practicable, the plant and piping layouts have been optimised to remove any areas where hydrogen could accumulate. Where the hydrogen concentration cannot practicably be kept to below 25% of the Lower Flammable Limit (typically where doing so would adversely affect functionality), measures such as explosion-resistant pipework and hydrogen leak detection are provided [Ref-18].
- The potential radiolytic hydrogen hazard in the Off-Gas (OG) system is managed by injecting steam to dilute hydrogen concentrations and using hydrogen recombiners to keep the hydrogen concentration far below its lower flammability limit (LFL). The hydrogen concentration is monitored at numerous points in the system and isolation takes place on detection of high hydrogen concentrations within pipework.
- The batteries used in the UK ABWR are the sealed type, which do not vent hydrogen. In addition, a Heating Ventilation and Air Conditioning (HVAC) system is installed in the battery areas.
- The hydrogen tank for cooling the main generator is stored in a separate building. The generator set and associated systems will incorporate appropriate provisions to minimise hydrogen fire risk.
- Storage tanks containing compressed flammable gases (hydrogen for calibration) have been designed and specified for the pressure and include relief valves, as per British Compressed Gases Association (BCGA) standards. The hydrogen concentration inside the storage buildings is below the explosive limit.
- High pressure oil system pipework is designed to prevent leakage and failure. This includes welded joints and complies with ASME Section III and B31.1 standards.
- High energy electrical systems are designed to include circuit breakers and other trip devices to prevent overpower from arcing faults. However, should the electrical protection fail the Class 1 divisional (and non-divisional) barriers are robust enough to prevent propagation of the fault to other Divisions.
- Areas containing hydrogen gas tanks and the battery rooms are actively ventilated to prevent the accumulation of an explosive atmosphere.
- Storage tanks and cylinders of combustible gases are stored either inside a locked area, or are restrained to a robust structure.
- Pipework systems are pressure tested during commissioning to ensure integrity. All systems are regularly inspected.
- The Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) are designed to protect workers from fire and explosion risks related to dangerous substances and potentially explosive or flammable atmospheres. At the site specific stage of design the future licensee will provide demonstration of compliance with DSEAR. This may include Hazardous Area Classification, a process which places strict controls on ignition sources in

areas with the potential for flammable or explosive atmospheres. Administrative rules with control the use, storage and handling of hazardous materials across the site.

7.4.3.6 Fire Protection

As per design requirement 3 in Section 7.4.3.3, the fire protection systems form a key part of the UK ABWR internal fire and explosion safety case. The divisional barriers provide the primary means of fire protection by limiting the effects of a hazard to a single division of A-1 SSCs. These are supplemented by the fire detection and suppression systems described in Sections 7.4.3.7 and 7.4.3.8 below that provide defence-in-depth by limiting the severity of any hazard that does occur. The fire detection and firefighting system features of the UK ABWR are described in detail in PCSR Chapter 16, Section 16.6.1 “Fire Protection Systems”.

It should be noted that the assessment of the design basis fire and explosion events does not take credit for the fire protection systems and they provide defence-in-depth against the loss of SSCs that deliver FSFs.

7.4.3.7 Fire Detection and Alarm Systems

Fire detection and alarm systems serve to detect a fire and provide warning to occupants in the vicinity of a fire and to the MCR. Detection and notification of a fire in an area containing SSCs delivering Fundamental Safety Functions allows operators to take action early in a fire scenario to mitigate the effects of the fire.

The assessment of the design basis fire and explosion events does not take credit for the fire detection and alarm systems and they provide defence-in-depth against the loss of SSCs that deliver FSFs.

7.4.3.8 Firefighting Systems

Automatic and manual fire suppression is provided for the UK ABWR as a defence in depth measure to limit the severity of fires. Where there is potential for rapid fire growth (e.g. pumps with large quantities of oil or diesel generator systems), fixed fire suppression systems are considered good practice and have been provided where appropriate. The fixed fire suppression systems are operated automatically and/or manually depending on local requirements.

The assessment of the design basis fire and explosion events does not take credit for the fixed fire suppression systems and they provide defence-in-depth against the loss of SSCs that deliver FSFs.

7.4.3.9 Firefighter Intervention

In some situations fires may be dealt with at an early stage of fire development by fixed fire suppression or manually by trained operators using fire extinguishing equipment. Where necessary and when it is safe to do so, firefighting services may enter UK ABWR buildings to deal with fires. The UK ABWR has the following features to allow firefighter intervention:

- The provision of vehicular access for fire appliances to the perimeter of the building or site.
- The provision of quick and easy entry to the interior of the building for fire brigade members and their equipment.
- The provision of access to sufficient supplies of firefighting materials.
- The means of enabling firefighters access to all areas of a building, including the provision of firefighting lifts if appropriate.
- The means of ensuring protected areas for firefighters to carry out their operations.
- The provision for fire and rescue service communications.
- The provision of facilities to release, or extract, smoke and heat from the building or site.
- The provision for removing firefighting extinguishing materials.

The assessment of the design basis fire and explosion events does not take credit for fire fighter intervention and it provides defence-in-depth against the loss of SSCs that deliver FSFs.

7.4.3.10 Combined Fire and Explosion Hazards

As per the definition in section 7.3.2.2 internal fires and explosions can be a cause of other consequential Internal Hazards. It is noted that the consequential combined events would only occur within the same division due to the divisional segregation provided by the UK ABWR design. The consideration of Combed Hazards is presented in the Topic Report on Combined Internal Hazards [Ref-14] and summarised in Section 7.16 (Internal Combined Hazards).

7.4.3.11 Mitigation of Fire and Explosion Hazards

The fire hazard analysis generally assumes that where there is a fire hazard, and where fire prevention and protection measures do not succeed in preventing or controlling the fire, then it may result in the loss of all equipment within the hazard compartment of origin. The approach to maintaining the Fundamental Safety Functions from internal fires is to then ensure that fires do not spread beyond that division to affect redundant equipment in other divisions; as discussed in Section 7.4.2 (underpinning internal hazard Claim IH_SFC_5.7-2).

For fires, this is known as the “Fire Containment Approach” to fire safety and is recommended in International Atomic Energy Agency (IAEA) Guide NS-G-1.7 [Ref-27] . The Fire Containment Approach relies on passive fire compartmentation and is highly reliable. The same concept can be applied to explosion events.

This is achieved by providing suitable barrier compartmentation between the different Class 1 divisions. The Class 1 divisional barriers (walls, floors and ceilings) that form the fire separation divisions are each designed to withstand the local and global effects of a design basis fire and are fully substantiated within [Ref-34].

Penetrations within Class 1 Barriers for human and equipment access routes and services are minimised as far as reasonably practicable and will be sealed with a material that will maintain the

classification of the barrier. The penetration seal will be rated to withstand a 3 hour fire and localised effects of fire and explosion.

Suitable fire dampers will be installed within HVAC ductwork that passes through a Class 1 Barrier. The length of HVAC ductwork between the barrier penetration and the damper will be fire rated to withstand the local effects of a 3 hour fire.

Where reasonably practicable, two sets of doors in series with an intervening lobby are provided in the Class 1 divisional barriers [Ref-16]. All doors or door systems within Class 1 Barriers will be fire rated to withstand the local effects of a 3 hour fire. A calculation of the front face temperature of the nearest divisional door exposed to a local hydrocarbon pool fire confirms that a single door is sufficient to maintain the divisional barrier and will be able to withstand the local fire effects of a bounding hydrocarbon pool fire [Ref-36].

For the majority of time both sets of doors will be closed, reducing the likelihood of the barrier being compromised by the performance of the door in the event of a postulated fire. The door monitoring system monitors the door position and alerts operators when the doors are left open. The door monitoring system has been classified based on the importance of the system to maintaining the Fundamental Safety Functions.

In some areas, the “Fire Influence Approach”, also described in IAEA Guide NS-G-1.7 [Ref-27] , is used to provide defence in depth against the consequences of severe fires (as described in Section 7.4.3.8), to protect commercial property and to meet conventional fire safety guidance. The Fire Influence Approach typically involves the use of fire protection equipment such as fixed fire suppression systems.

The explosion hazard analysis generally assumes that where there is an explosion hazard, it results in the loss of all equipment within the hazard compartment of origin. The robust, reinforced concrete divisional barriers are claimed to contain the effects of any internal explosion to a single division of A-1 SSCs. For explosion hazards the most severe effects occur on very short timescales and therefore the focus is on explosion prevention and containment rather than mitigating its effects. The Class 1 divisional barriers (walls, floors and ceilings) that form the fire separation divisions are each are fully substantiated to contain the effects of any internal explosion to the division of origin [Ref-34].

7.4.4 Safety Evaluation

7.4.4.1 General Approach to Fire and Explosion Consequences

A fire or explosion event has the potential to not only damage all the SSCs in the division of origin but also spread through internal walls and damage SSCs in multiple divisions. Therefore, when no account is taken for hazard compartmentation, the impact of an internal fire hazard event on the safety classified SSCs is assumed as the failure of all safety classified SSCs from all Class 1 divisions, thus threatening the delivery of the FSFs. When compartmentation is claimed as

containing the effects of a fire event, it is assumed that this only prevents the Internal Hazard effect from spreading beyond the division of origin. The SSCs within the division of origin are assumed to be lost in any fire/ explosion event in the same division.

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with hazard compartmentation barriers (see Section 7.3.1.9); in the case of the PCV, the MCR and the MSTR, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively. There are a limited number of additional cases where it is justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment, these exceptions to segregation have been assessed in [Ref-25], where it has been demonstrated that the FSFs can still be delivered following an internal fire and explosion hazard.

7.4.4.2 Consequences of fire or explosion during power operation

The fire prevention and protection measures in Sections 7.4.3.5 to 7.4.3.9 limit the frequency and severity of fires and explosions. In the unlikely event of a fire/ explosion, the consequences are limited to a single division of A-1 SSCs by Class 1 divisional barriers between the source of the fire/ explosion and the A-1 SSCs.

When considering the effects on the Class 1 divisional barriers from fires, it is important to consider both the global and local effects of the fire. The Detailed Analysis of Fire Modelling and Barrier Response report [Ref-36] confirms that a 3hour fire bounds the worst case design basis global internal fire hazards for all safety classified buildings within the UK ABWR, whilst a hydrocarbon pool fire bounds the local fire effects for all safety classified buildings within the UK ABWR.

High energy arcing faults (HEAF), oil mist and Hydrogen are identified as credible explosion hazard sources in a number of the safety classified buildings. These explosion hazards have been quantified and analysed for each affected building in [Ref-36].

The Class 1 divisional barriers, and their associated penetrations, are fully substantiated within the Barrier Substantiation Report [Ref-34] to contain the effects of a fire or an explosion to the division of origin.

Whilst FSFs can be supported by the remaining divisional A-1 and A-2 SSCs, Normal Operations (NO) SSCs may be lost during the fire or explosion hazard. The bounding loss of NO SSCs is during a LOOP, therefore LOOP is treated as the bounding fault for fire and explosion hazards during power operations. Depending on the plant technical specifications to be determined during detailed design, the loss of A-1 or NO SSCs during a fire of explosion hazard may lead to the requirement to shut down the reactor. The Class 1 divisional barriers ensure that suitable and sufficient A-1 and A-2 SSCs are protected from the fire or explosion hazard and will remain available to achieve cold shutdown and the other FSFs.

7.4.4.3 Consequences of fire or explosion during outage

For the maintenance and replacement of some larger equipment it is necessary to open hatches within floor slabs, some of which are part of Class 1 divisional barriers. Whilst the detailed outage schedule has not been confirmed at this stage, account has been taken for the possibility that such hatches will remain open throughout significant periods of the outage operations. This reduces the extent of divisional compartmentation provided between A-1 SSCs of different divisions in some stages of outage. However, assessments of available systems in outage show that there remain suitable and sufficient A-1 and A-2 SSCs during an Internal Hazard in any phase of outage to deliver the FSFs, this includes the Class 2 FLSS, Class 2 HWBS. In addition a range of Class 3 systems including FLSR, MUWC and SPCU are also available. The Hazard Schedules for fire and explosion hazards [Ref-2] detail all available safety systems following such events.

7.4.5 ALARP Discussion

The UK ABWR fire protection philosophy ensures the delivery of the FSFs primarily through the use of the Class 1 fire resisting barriers. This approach follows good practice for modern-standard buildings in the nuclear industry.

Prevention and protection measures have been implemented in the UK ABWR design to limit both the likelihood of a fire/ explosion event and the severity of fire/ explosion events. Provision of these prevention and protection measures has followed good practice/ modern standards with the choice of these measures addressing defence in depth and a hierarchical approach.

The UK ABWR design also includes a number of defence in depth systems and arrangements to ensure that fires within divisions will not easily spread and the risk of an internal fire and explosion is lowered to ALARP. Systems include Safety Class 3 Fire Detection and Alarm Systems, Smoke Control Systems, Manual Firefighting Systems, and some Fixed Fire Suppression Systems.

Internal walls, ceilings and floors that do not form the Class 1 fire barriers at the boundary of hazard compartments are not claimed as formal mitigation. However, these walls, ceilings and floors provide additional defence-in-depth protection from, and mitigation of, the effects of internal fire hazards.

With respect to Internal Fire and Explosions, it is concluded that all reasonably practical risk reduction measures have been implemented and that the risks due to internal fire and explosion hazards are considered to be ALARP.

7.4.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of fire and explosion hazards, prevent fires and explosions from occurring, and limit the severity and impacts on equipment from fires and explosions. The design also provides adequate segregation for the redundant and diverse equipment required to maintain the Fundamental Safety Functions in the

case of an internal fire or explosion. The redundant and diverse equipment is protected by robust Class 1 divisional barriers that are capable of resisting the potential fire and explosion hazards.

The fire and explosion hazard analysis [Ref-2] has demonstrated that the UK ABWR is designed so that any internal fire or explosion within the design basis will not compromise the Fundamental Safety Functions.

7.5 Internal Flooding

7.5.1 Introduction

The Topic Report on Internal Flooding [Ref-3] considers immersion, water spray and steam release hazards. Internal flooding can occur due to leakage from pipes or vessels containing a fluid, including general cooling water services, reactor feedwater, condenser cooling water supplies, oil and chemical reservoirs.

Steam releases may occur due to leakage from steam pipes or flashing off from of a release of superheated water. Condensing steam is also considered to be a secondary source of flooding.

Internal flooding is postulated to occur randomly from the above sources, and may result from another Internal Hazard.

A comprehensive Hazard Schedule, containing all bounding flooding hazard events identified, is presented within the Topic Report on Internal Flooding [Ref-3]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.5.2 Claims and Arguments

As for all other Internal Hazards, the principal means of mitigating internal flooding hazards is through the containment of the effects of the hazard within the division of the initiating event using barrier compartmentation. This is summarised in the general claims for Internal Hazards made within Section 7.3.1.5.

Specific to the flooding and steam release hazards is the requirement for engineered pathways to route flood water or steam from its source to a preferred location, these pathways determine the maximum credible loads on the divisional barriers. In addition, the flooding safety case accepts the immersion of multiple divisions in the B3F levels of the Reactor Building (R/B) and Control Building (C/B) provided that specific SSCs are protected by suitable non-divisional barriers or are qualified for immersion.

These requirements lead to the following safety claims and arguments specific to flooding. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH_F_SFC_5-7.1: General internal flooding claim
Any internal flood event within the design basis will not prevent delivery of the Fundamental Safety Functions.

This and the general high level claims are then supported by lower level more detailed claims and arguments below which together demonstrate the higher level claims have been achieved. This provides an auditable and logical process for demonstrating that the design intent has been achieved.

These are derived utilising experience, engineering judgment and the safety philosophy/approach to hazards discussed in Section 7.3.1, applied to the UK ABWR design.

Claim IH_F_SFC_5-7.2: Limiting Flooding to a single Class 1 division
The Class 1 divisional barriers segregating neighbouring divisions will be such that the consequences of a design basis flooding event in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

(IH F SFC 5-7.2.A1)
For buildings containing Class 1 equipment, redundant divisions of equipment are segregated by Class 1 Divisional barriers which function as flood barriers. The approach to barrier substantiation is presented within Section 4 of the Barrier Substantiation Report [Ref-34].

For the purpose of internal flooding, the functional intent of divisional barriers is to protect against the consequence of a flooding hazard event, such that the consequences will not undermine the function of Class 1 SSCs in any neighbouring division. This is achieved in general by limiting the flooding event to the division in which the flooding event originates. The loss of one such division of equipment is generally considered to be acceptable. Acceptability of such events, is demonstrated in the Hazard Schedule of Internal Flooding, Section 14 of [Ref-3].

Exceptional flood paths, which have the potential to challenge multiple divisions, are located in the following areas:

- Exception 1 - Reactor Building (R/B), B3F level (-20500)
- Exception 2 - Control Building (C/B), B3F level (-23000)

The consideration of these exceptions is detailed in ***IH_F_SFC_5-7.3.1***.

(IH SFC 5-7.2.A2)
Within a division, engineered features (doors gaps, hatches, blowout panels, penetrations and stairwells) are used to route flood water or steam to a preferred location. Flood paths are discussed further in Section 7.5.4.2. The detailed description of flood paths is presented within the Evidence Report for Internal Flooding [Ref-33].

(IH SFC 5-7.2.A3)
A Flood originating in buildings not containing Class 1 equipment does not propagate to buildings which do contain Class 1 equipment.

Claim IH_F_SFC_5-7.3: Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after the internal flood, to fulfil the Fundamental Safety Functions.

Exceptions to Segregation are defined as Safety Classified A-1 Systems, Structures or Components (SSCs) from different safety divisions which are located in the same hazard compartment, or Safety

Classified A-1 and A-2 SSCs which are located in the same hazard compartment. Identification and Characterisation of Exceptions to Segregation is provided in the Topic Report on Exceptions to Segregation [Ref-25].

(IH F SFC 5-7.3.A1 & IH F SFC 5-7.3.A2)
Exception to Segregation SSCs vulnerable to failure from flooding or steam release are, where possible, designed to fail safe. In addition, alternative means of delivering the FSFs exist for all exception to segregation SSCs. As demonstrated in [Ref-25], these alternative means of delivering the FSFs are not vulnerable to the original flooding or steam hazard.

Prevention and protective measures are incorporated into the design to protect the delivery of Category A safety functions from the effects of flooding. Flooding Prevention and Protection features are discussed in further detail in Sections 7.5.3.6 and 7.5.3.7 respectively.

In addition to the Exceptions to Segregation as defined above, the following exceptions to divisional segregation are considered for flooding events:

Claim IH_F_SFC_5-7.3.1: Where flooding affects multiple Class 1 divisions, protection features such as non-divisional flood barriers or qualification of individual SSCs will be such that the consequences of a design basis flooding event in one division will not prevent SSCs in neighbouring divisions delivering their fundamental safety functions.

For the following areas within the Reactor Building and Control Building, engineered flood paths exist which result in flooding in multiple Class 1 divisions. This is limited to the following:

- Exception 1 - Reactor Building (R/B), B3F level (-20500)

  A design basis flooding event which is capable of flowing to the R/B B3F level has the potential to flood the corridor areas, provided there is sufficient flood water/steam released. This corridor area consists of several connected rooms, which are located across multiple safety divisions. Rooms linked to the corridor are connected by doors, some of which do not have any claimed flood protection rating. The corridor area is detailed within the Topic Report on Internal Flooding [Ref-3]. The flood will progress through the corridor via engineered openings and into non-flood protected rooms via adventitious openings.

  For flooding events which result in propagating to this corridor area, there is the potential to affect other connected rooms, including those containing A1 SSCs. Rooms containing ECCS equipment are protected from flooding events originating in other divisions by additional non-divisional Class 1 flood barriers and doors. Any required function provided by ECCS equipment, will not be challenged by a flooding event and the equipment affected is limited to a single division of equipment. Bounding flooding events which require such barriers, are detailed in the Hazard Schedule presented within Section 14 of the Topic Report on Internal Flooding [Ref-3]. Substantiation of these features is presented within the Barrier Substantiation Report [Ref-34], Section 5.

- Exception 2 - Control Building (C/B), B3F level (-23000)

  A design basis flooding event which is capable of flowing to the C/B B3F level has the potential to affect all rooms at this level, provided there is sufficient flood water/steam released. This therefore results in flooding in multiple safety divisions. This level of the Control Building contains no A1 SSC. The consequences of such a design basis event are determined to be acceptable, as no fundamental safety functions are challenged.

7.5.3 Design Basis

7.5.3.1 Flooding Analysis Methodology

The assessment for immersion flooding hazard has been performed based on the following approach:

(1) Identification of flooding sources (pipework, vessel, etc.) within each room or area.
(2) Identification of the systems associated with the flooding source (e.g. Condensate Storage Tank or Suppression Pool) to determine the maximum volume of flood water available.
(3) Identify the safety significant SSCs that require protection against the flooding hazard.
(4) Evaluation of the amount of flood water which can be released from the identified flooding sources.
(5) Analysis of the flood progression in each room or area.
(6) Identification of flooding compartments claimed to contain flood water and prevent propagation into other Class 1 divisional areas.
(7) Identification of flooding paths through doors, hatches, connected ducts and pipe penetrations.
(8) Identification of all the detection and alarm systems for determining the location of the flood.
(9) An assessment of the acceptability of flood depths is performed.

In the majority of cases, the consequences of a spray release are considered to be bound by the immersion flooding case for each room/area. However there may be SSCs located above the maximum flood height that may still be vulnerable to a spray release. Where this has been identified the following methodology has been applied.

(1) Identification of potential sources of spray within each room or area.
(2) Determination of any spray scattering zones and identification of obstacles between spray source and SSCs.
(3) Quantification of potential spray release.
(4) Identify the safety significant SSCs that may be damaged by the spray release.
(5) Identification of mitigation features.
(6) An assessment of the consequences of a spray release.

The assessment for steam release hazard has been performed based on the following approach:

(1) Identification of potential steam sources.

(2) Identification of steam compartments.
(3) Identify the safety significant SSCs that may be damaged by the steam release.
(4) Identification of steam release path.
(5) Quantification of potential steam releases.
(6) Identification of mitigation features.
(7) An assessment of the consequences of a steam release.

These methodologies are consistent with Section 7.2.1, including the further detail presented in section 7.3.1, and designed to demonstrate that suitable and sufficient A-1 and A-2 SSCs will remain available to deliver the FSFs following an internal flood hazard in the UK ABWR.

All buildings have been assessed to determine whether a flood progression can result in SSCs in one building being affected by flooding originating in another. The detailed list of affected systems is shown in the Hazard Schedule of Internal Flooding [Ref-3].

7.5.3.2 Assessment Assumptions

The following assumptions provide the basis for assessing postulated flooding hazards:

- Flooding is initiated by failure of a pipe, valve, or vessel.
- Pipework or vessel failure can occur in any pipe or vessel on the site except the RPV and very high integrity components, where special high integrity arguments apply.
- Only a single pipework failure takes place at any given time. Secondary pipework failure is not considered as the consequences of flooding cannot induce pipe failure. Pipe whip events that cause secondary pipework failures are considered to be a combined hazard and are considered in the Topic Report on Combined Internal Hazards [Ref-14].
- All pipe failures are considered to be full bore breaks for design basis assessments unless otherwise justified.
- Pipe or vessel failure may occur at any time during power operation or during shutdown.
- Pipe or vessel failure may occur as a result of another internal/external event.
- Multiple pipework and vessel failures caused by a single event such as earthquake or pipe whip may occur. Note that pipe whip failure is dealt with as a separate hazard.
- Where pipework is connected to valves, pumps, turbines or vessels, failure of these plant items are assumed to be bounded by failure of the connected pipework.
- As the supply pipe is the source of flooding the failure of other plant items (e.g. valve, pump, etc.) is considered to be bounded by the connected pipework.
- The impact to barriers by any dynamic wave effects of sudden water release are judged to not be greater than the bounding hydrostatic effects.

The assumptions for the spray assessment are as follows:

- Spray is considered to occur from a through wall crack in any pressurised water pipework.
- Components that are qualified to a suitable spray specification are assumed not to fail.

The assumptions for the steam release assessment are as follows:

- Sources of steam release are high temperature water and steam pipes (>100°C).
- The steam released will spread throughout the room where the break occurs and to other areas through the room penetrations (which may be engineered routes). These penetrations are assessed as part of the steam release study.
- Increased humidity is assessed.
- All unprotected and unqualified components are assumed to fail following contact with steam.
- The duration of steam release is assumed to be until isolation occurs.
- The provision of manual and automatic actions upon detection of a pipe break e.g. stopping pump for the system, closing isolation valves.

During outages when maintenance operations are in place, hatches may be opened to facilitate access of personnel and equipment, therefore challenging compartmentation. The following assumptions are made for the outage assessment:

- During outages it is assumed that the requirements for the FSFs are less onerous due to the control rods being fully inserted and the decay heat is less than at power modes. The relevant FSFs are therefore long term cooling (FSF3) and Others (FSF5).
- Where equipment is moved through divisional Class 1 barriers, the doors will be opened only temporarily and will be closed immediately after passage.
- Hatches may be left open for one to two days. Therefore, it is assumed that the associated Class 1 divisional barriers are compromised during this period.
- Temporary services are not ran through doors during normal outage operations. This will only be done during plant modifications therefore it is not considered that these doors may be open as part of GDA.
- For all hazard scenarios that require initiation of FLSS, it is assumed that the FLSS is manually initiated to deliver the FSFs during outage (PCSR Chapter 27, Section 27.6.3).

During the site specific stage, once the detailed outage schedule is available, the deterministic assessment for internal flooding hazards during outages can be revised as necessary by the future licensee.

7.5.3.3 Design Requirement

The internal flooding claim in Section 7.5.2 has been achieved in the UK ABWR by:

- **Limiting flooding sources**. The number of flooding sources is limited as far as possible by routing pipework to areas not susceptible to flooding and reducing the number of large water sources.
- **Prevention of pipe and vessel failure**. Piping and vessels are designed and qualified for the anticipated hydrodynamic loads and environmental conditions.

- **Reduction in the quantity of flood water, or reduction in flood heights to acceptable levels**. Potential flood source volumes are minimised as far as reasonably practicable, flood management features are incorporated into the design to route flood water through defined flood paths.
- **Mitigation of the consequences of severe flooding**. Barriers are qualified for the anticipated flood heights and equipment is qualified (to continue to operate or fail safe) for immersion where required.

7.5.3.4 Sources of Internal Flooding Hazards

Sources of Immersion and Water Spray

There are a number of large water sources that can affect safety classified buildings in the UK ABWR design. These are:

- Circulating Water System (CW)
- Condensate Storage Tank (CST)
- Emergency Equipment Cooling Water System (EECW)
- Flooder System of Specific Safety Facility (FLSS)
- HVAC Normal Cooling Water System (HNCW)
- HVAC Emergency Cooling Water System (HECW)
- Heating Steam and Condensate Water Return System (HSCR)
- Make Up Water Condensate System (MUWC)
- Make Up Water Purified System (MUWP)
- Reactor Building Cooling Water System (RCW)
- Reactor Building Service Water System (RSW)
- Spent Fuel Storage Pool (SFP)
- Standby Liquid Control System (SLC)
- Suppression Pool (S/P)
- Turbine Building Cooling Water System (TCW)
- Turbine Building Service Water System (TSW)

Sources of Steam Release

There are several sources of steam release during power operation or shutdown modes:

- Heating Steam System (HS) and Heating Steam and Condensate Water Return System (HSCR),
- Main Steam System (MS),
- Reactor Water Clean-up System (CUW),
- Reactor Core Isolation Cooling System (RCIC),
- Feedwater System (FDW).

7.5.3.5 Bounding sources of Internal Flooding

These flooding sources are considered to bound the flooding effects from other, lesser sources. The following sections present the sources which are consider to bound the effects within buildings containing Class 1 SSC's, and therefore have the potential to affect Fundamental Safety Functions. Acceptability of hydrostatic loadings of required barriers for these cases are presented within the Barrier Substantiation report [Ref-34]. All bounding sources are detailed in the Topic Report on Internal Flooding [Ref-3].

Reactor Building

Within the Radiation Controlled Area (RCA) of the building, the combination of the CST and S/P flood sources is considered to be the credible single failure, which results in the largest hydrostatic loading of barriers. This flood volume is contained within the basement annulus of the R/B as detailed by Exception 1.

Within the Non-RCA of the R/B, the credible flood source which results in the largest hydrostatic loading is the MUWP and is limited to a single division by divisional barriers.

Heat Exchanger Building

The credible flood source which results in the largest hydrostatic loading within the Hx/B is the TSW. The consequences of a flood from this system results in a challenge to divisional barriers from the non-divisional side of the barrier only, flooding cannot affect safety divisional areas. Within the safety divisional areas of the building, the bounding flood source is the RSW. Any single credible flooding event initiated by a RSW line break, will result in flooding within a single safety divisional area only.

Control Building

The combination of the RCW source is considered to be the credible single failure, which results in the largest hydrostatic loading of barriers. This flood volume is contained within the B3F level of the C/B as detailed by Exception 2 in section 7.5.2.

Turbine Building

The CW is the bounding flood source in the T/B and will affect the T/B and yard areas only. There are consequences from flood water in the T/B or yard. Connections between the T/B and other buildings are not challenged by the largest credible hydrostatic loading.

Emergency Diesel Buildings

The RCW is considered to be the credible single source for each EDG/B, which results in the largest hydrostatic loading of barriers. The three EDG/Bs are physically segregated and a flood in one EDG/B does not affect the other buildings.

Service Tunnels

The routing of the Service tunnels are not defined in GDA therefore it is conservatively assumed that the flooding event fills the ST from the floor to the soffit (a flood event that completely fills the ST). The flood water height within the ST therefore equals the internal height of the ST.

7.5.3.6 Flood Prevention

UK ABWR includes a number of design features that minimise the probability of a flood from occurring inside the plant:

- Pipes and vessels have mostly welded joints and are designed to ASME and American National Standards Institute (ANSI) standards (See Section 5.8 of this PCSR Chapter 5 'Applied Regulations, Code and Standards').
- Most safety classified pipes and vessels (which contain the largest flooding sources) will be part of the Examination, Maintenance, Inspection and Testing (EMIT) schedule and will have periodic inspections according to ASME Sections V and XI (as appropriate).
- Pipework systems and vessels are pressure tested during commissioning to ensure integrity and all pressurised systems are designed with suitable overpressure protection to comply with UK legislation as a minimum.
- The materials and chemical control specified for pipework systems and components ensure corrosion or other failure mechanisms are minimised throughout the design life of the component or system.

7.5.3.7 Flood Protection

In order to reduce the amount of flooding, isolation valves are provided to isolate pipe and vessel failures. This isolation can be initiated automatically, or it can be manually actuated, either from the MCR or locally. The reduction in the flooding volume depends on the leak rate and the time required to close the isolation valves. The leak rate and duration time is conservatively assessed and depends on:

- Interlocks to automatically close the isolation valves.
- Leak detection to alert operators and indicate the locations of leaks.
- Remote or manual operation of the isolation valves (subject to a Human Factors assessment).

Leak detection and alarm systems in sumps and drains serve to detect the presence of fluid leakage and provide warning to operators locally to the flood and in the MCR. Leak detection may also automatically actuate isolation. Detection and notification of the existence of flooding in an area containing SSCs that perform a Fundamental Safety Function allows operators to take actions to mitigate the effects of flooding.

It is recognised that full bore breaks from large flooding sources may not be recognised in time for manual isolation of the flood source. However, the above mitigation measures allow a graduated approach to the flooding hazard.

It should be noted that the assessment of the design basis flooding events does not take credit of sumps and drains to enable a highly conservative assessment to be completed which results in a large margin of safety. Although it is acknowledged that the measures listed above provide defence in depth against the loss of equipment that deliver Fundamental Safety Functions.

7.5.3.8 Combined Hazards

As per the definition in section 7.3.2.2 and assessment in Section 7.16, a flood can be a cause of other consequential Internal Hazards. The consideration of Combined Hazards is presented in the Topic Report on Combined Internal Hazards [Ref-14].

7.5.3.9 Mitigation of Flooding Hazards

Mitigate Consequences of Severe Flooding

If all the flood prevention approaches described above were to fail, the general approach to ensuring protection of SSCs of the Fundamental Safety Functions is to limit the impacts of an internal flood to within one Division.

In addition, the UK ABWR design uses pedestals to raise safety classified equipment above the floor, which provides protection against flood levels below the pedestal height. Where required additional mitigation is specified, including the use of equipment qualified for immersion.

In the R/B and C/B large flood sources are allowed to spread through engineered penetrations to specified flood areas. The detailed design of these penetrations will not be confirmed until the site specific phase however any engineered flood penetrations will also be qualified to prevent spread of other hazards (e.g. fire). Protection is provided by water tight doors and by qualifying structures to the maximum design hydraulic pressure levels as a result of a flood.

7.5.4 Safety Evaluation

7.5.4.1 General Approach to Immersion, Spray and Steam Consequences

The UK ABWR is designed to prevent an internal flood from occurring. However if an internal flood does occur, the overall plant design with respect to the effects of flooding is to assume a full bore break of the pipework, and that all equipment within the division affected by the flood has failed. Redundant equipment in other divisions required to maintain the Fundamental Safety Functions is protected by appropriately designed barriers. The Flooding Hazard Assessment evaluates the compliance of the design against this requirement for redundancy.

Identification and characterisation of flooding events is provided in the Topic Report of Internal Flooding, including Immersion, Spray and Steam Release [Ref-3], and a number of design basis events have been derived. The bounding set of design basis events have been derived using the Flooding Analysis Methodology (as per Section 7.5.3.1).

Where divisional barriers are identified to be challenged by a bounding event, the barriers and any penetrations are demonstrated to be able to withstand the loads imposed by flood water or steam pressure without structural collapse or excessive leakage. The substantiation of these barriers is provided in the Barrier Substantiation Report [Ref-34]. The structural integrity of divisional structures and penetrations is assessed via consideration of their bending moment and shear force capacity. The substantiation demonstrates that the protection features are robust, and therefore no more than one safety division can be challenged by a single flooding event.

For buildings which do not contain Class 1 SSCs, all functions provided by equipment in the building may be affected by a flooding event. No fundamental safety function can be challenged by such an event, and no prevention or protection are required. Any prevention and protection features in these buildings are considered as defence in depth measures only.

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with flood barriers (see Section 7.3.1.9); in the case of the PCV, the MCR and the MSTR, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively. There are a limited number of additional cases where it is justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment, these exceptions to segregation have been assessed in [Ref-25], where it has been demonstrated that the FSFs can still be delivered following an internal flooding hazard.

Whilst the detailed outage schedule has not been confirmed at this stage, it is conservatively assumed that both movement of equipment and running of temporary services through the divisional Class 1 barriers will lead to a compromising of the divisional compartmentation during the outage. Over the course of the outage a series of new flood compartmentation configurations occur that compromise the Class 1 divisional segregation claimed for power operations. The outage progresses through five distinct Plant Operating States and two main phases where Class 1 divisions are alternately taken out of service for maintenance. The consequences of a flood during outage is discussed in Section 7.5.4.4 below.

7.5.4.2 Flood Water Paths

Flood water is expected to propagate both horizontally throughout the level on which the pipe rupture occurs as well as vertically between levels. Within Class 1 buildings, flooding is limited both horizontally and vertically, to the safety division of origin. While it is typical for flooding to proceed to lower levels, it is also possible for flooding to affected higher levels through back flow processes when all available space on the lower level(s) has become flooded. Flood propagation from the room of origin considers the following paths:

- Door gaps
- Stairwells/elevator shafts
- Penetrations (e.g. cable tray or piping which are not sealed),
- Floor gratings, weirs and unsealed ladder and hatch openings.

Various door types are present throughout the design and their influence on flow are as follows:

- Physical barriers which obstruct the flow between adjacent safety divisions (e.g. standard door, steel door). Where present, the flow to an adjacent division is assumed to be through a door gap present at the base of the door, and is minimal.
- Watertight doors which are assumed to be conservatively closed which in turn increases the water heights in adjacent areas for flooding originating outside these rooms.

Stairwells, elevators and hatches provide an opportunity for flooding to proceed vertically between different levels. Although the room itself may flood, stairwells and elevators are treated as conduits through which flooding propagates to other areas of the plant. Hatches exist throughout the design for lifting equipment between vertical levels and provide conduits through which flooding propagates vertically. In addition, flooding hatches have been engineered into the design to limit flooding to a single safety divisional area.

The non-divisional flood barriers are designated as Safety Class 1 (consistent with the Class 1 designation of the divisional barriers). The substantiation of these barriers is provided in the Barrier Substantiation Report [Ref-34].

7.5.4.3 Consequences of Immersion and Spray during Power Operation

All A-1 SSCs include three redundant mechanical divisions and four redundant C&I divisions. During power operations the SSCs which belong to one Class 1 division are physically segregated from other redundant divisions by Class 1 divisional barriers. These barriers create flood compartmentation and pathways that, in the event of a large leak, route water through the same division. Smaller leaks remain in the room of origin or overflow to adjacent rooms within the same Class 1 division.

In the case of the R/B, the Basement Annulus (B3F level) has been identified as an exception to divisional segregation (Exception 1), as the flood water is designed to pool in the Basement Annulus and therefore may breach three of the four Class 1 divisions in the basement level. Division IV equipment is isolated within flood protected rooms. The distribution of equipment within the R/B basement is such that ECCS components can only be challenged within a single division at most. This is achieved using flood protected rooms for such equipment. Substantiation of these features is presented within the Barrier Substantiation Report [Ref-34], Section 5.

With regards to CRD equipment, the system design is fail-safe and therefore no A-1 function of this system can be undermined; see PCSR Chapter 12: Reactor Coolant Systems, Reactivity Control Systems and Associated Systems, Section 12.4.3.1 for more details on the CRD equipment.

All other A1 equipment susceptible to a flooding event, is qualified to withstand the design basis event, such that all Fundamental Safety Functions are not compromised; see the Design Substantiation sections of the Topic Report of Internal Flooding [Ref-3].

In the case of the C/B, the lowest floor (B3F level) has been identified as an exception to divisional segregation (Exception 2), as the flood water is designed to pool in all rooms at this level and therefore may breach three of the four divisions in the basement level. This floor level of the Control Building contains no A1 SSC. The consequences of such a design basis event are determined in Appendix C of [Ref-3] to be acceptable, as no fundamental safety functions can be challenged in multiple divisions.

In the case of the Hx/B, a flooding event originating at the B1F level is retained within the safety division of origin, or in case where the flood event originates in a non-divisional area the flood event does not pass into a safety division. All flood sources that originate above B1F level are directed to flow down into a flood compartment at B1F level, via an engineered pathway. Each flood compartment on B1F level is specific to a particular safety division or otherwise represents a non-divisional area. All flood volumes are retained within their originating safety division or are otherwise retained within a non-divisional area. To ensure that the divisional barriers within the B1F level are capable of withstanding the hydrostatic loads, a small increase in wall thickness and reinforcement has been incorporated into the design (see [Ref-34], Section 8).

7.5.4.4 Consequences of Immersion and Spray during Outage

As the detailed outage schedule will be provided by the future licensee at site specific stage, it has been necessary to make a set of highly conservative assumptions as part of the outage deterministic assessment. In particular, where hatches are required to be open to allow movement of equipment, these are assumed open during that phase of the outage. Some hatches pass through multiple divisions. This reduces the extent of divisional compartmentation provided between A-1 SSCs of different divisions in some stages of outage. However, assessments of available systems in outage show that there remain suitable and sufficient A-1 and A-2 SSCs during an Internal Hazard in any phase of outage to deliver the FSFs, this includes the Class 2 FLSS, Class 2 HWBS. In addition a range of Class 3 systems including FLSR, MUWC and SPCU are also available. The Hazard Schedule of Flood events [Ref-3], details all available hazard safety systems following such events.

There is a specific outage related flooding hazard originating within the PCV that, if unmitigated, could lead to consequential flooding within the Reactor Building. Sufficient counter-measures will be in place such that flood water will be contained within the drywell of the PCV, see Section 7.12 for further details.

7.5.4.5 Steam Release Paths

Steam is expected to propagate both horizontally throughout the level on which the pipe rupture occurs as well as vertically between levels. Within Class 1 buildings, the steam release is limited to a

defined route within the safety division of origin. Steam propagation from the room of origin to the outside atmosphere along the defined route is dependent on the following features:

- Engineered Penetrations,
- Adventitious Penetrations (e.g. HVAC ductwork and unsealed piping), and
- Blow Out / Rupture Panels.

7.5.4.6 Consequences of Steam Release

The most significant consequences from steam release arise from the MS, RCIC and CUW systems. The high temperatures and pressures of these systems result in a rapid pressure rise in the room of origin followed by a fast reduction in pressure as the steam sources are isolated and the pressure relief to atmosphere via the engineered steam release path occurs. The steam release paths ensure that the divisional segregation is maintained and that, consistent with the immersion flooding described above, suitable and sufficient A-1 and A-2 SSCs remain available to deliver the FSFs. The substantiation of the barriers forming the steam release path is provided in the Barrier Substantiation Report [Ref-34].
Pipework belonging to the Heating Steam System (HS) and the Heating Steam Condensate Water Return System (HSCR) is largely excluded from areas which are classed as safety divisions. In addition, instances where HS pipework is routed through safety divisional areas, the engineered steam path for RCIC is used and additional engineered steam path will be installed as necessary. Therefore, the HS and HSCR are not deemed to be credible sources of Steam Release.

7.5.5 ALARP Discussion

There are a number of large water sources that can affect safety classified buildings in the UK ABWR design, the volumes held by these sources of Internal Flooding have been minimised as far as reasonably practicable whilst still ensuring that they are able to deliver their required safety functions. In accordance with relevant good practice, piping and vessels are designed and qualified for the anticipated hydrodynamic loads and environmental conditions they will experience. In addition, features are incorporated into the design to route flood water or steam through defined paths to preferred locations. Whilst not credited in the design basis assessment, engineered systems are available to allow early detection and termination of a potential flood. With respect to Internal Flooding, it is concluded that all reasonably practicable risk reduction measures have been implemented and that the risks due to Internal Flooding Hazards are considered to be ALARP.

7.5.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of the internal flooding hazard, and to prevent floods from occurring. The design also provides for redundant and diverse equipment to maintain the Fundamental Safety Functions in the case of an internal flood event, which includes spray and steam release events.

This redundant and diverse equipment is protected by robust barriers that have been shown to withstand the design basis flood conditions. The internal flooding hazard assessment completed during GDA Step 4 demonstrates that the UK ABWR is designed so that any internal flood event within the design basis will not compromise the Fundamental Safety Functions.

7.6 Pipe Whip and Jet Impact

7.6.1 Introduction

The Topic Report on Pipe Whip and Jet Impact [Ref-4], considers the local dynamic hazards of pipe whip and jet associated with the failure of pressurised parts.

As discussed in [Ref-4], pipe whip occurs when a high energy pipe fails in a guillotine manner and the resulting energy release causes the pipe to whip. Where this is the case there will also be a jet of fluid from the two ends of the broken pipe. Jets can also occur from pipe failures that do not involve guillotine failures, but these effects will be less severe than those from guillotine failures. The whipping pipe or the fluid jet may impact safety classified equipment near the pipe failure.

A comprehensive Hazard Schedule, containing all bounding pipe whip and jet hazard events identified, is presented within [Ref-4]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCR Chapter 24 'Design Basis Analysis'.

7.6.2 Claims and Arguments

As for all other Internal Hazards, a principal objective of the pipe whip and jet safety case is to demonstrate the effects of any pipe whip or jet hazard are limited to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5. Appendix A presents the full claims table for this PCSR Chapter; no hazard specific claims are required for pipe whip and jet hazards, however the following hazard specific arguments have been developed in support of claim IH_SFC_5-7.2:

(IH_PJ_SFC_5-7.1.A1)
Pipe whip and jet impact assessments are performed for all high energy pipes operating at a temperature greater than 95ºC and/or a pressure of greater than 1.9 MPa (gauge) to determine their damage potential to SSCs that deliver FSFs.

Further details on the characteristics of the sources of pipe whip and jet impacts can be found in Section 7.6.3.4 below, whilst Section 7.6.3.5 discusses the preventative measures incorporated into the UK ABWR design that significantly reduce the likelihood of pipe whip and jet impact hazards.

(IH_PJ_SFC_5-7.1.A2)
For buildings containing multiple redundant divisions of Class 1 equipment, the divisions are segregated by Class 1 divisional barriers of sufficient integrity that pipe whip events are contained to the division where they originate (i.e. the pipe whip does not perforate the barrier).

The approach to barrier substantiation against pipe whip and jet impacts is presented within Section 4 of the Barrier Substantiation Report [Ref-34], whilst demonstration that all identified barriers do not perforate following a pipe whip or jet impact is presented in Section 5 of [Ref-34].

(IH_PJ_SFC_5-7.1.A3 & IH_PJ_SFC_5-7.1.A4)
Equipment layout ensures that any secondary effects from an internal pipe whip event in one division (e.g. concrete scabbing) will not initiate a hazard event in a different division, and there will be sufficient SSCs in the other divisions available to deliver the Fundamental Safety Functions.

Demonstration that scabbing of barriers does not initiate a hazard or prevent SSCs in an adjacent room from delivering their required safety functions is presented in Section 5 of [Ref-34].

(IH_PJ_SFC_5-7.3.A1 & IH_PJ_SFC_5-7.3.A2)
Exception to Segregation SSCs vulnerable to failure from pipe whip & jet are, where possible, designed to fail safe. In addition, alternative means of delivering the FSFs exist for all exception to segregation SSCs. As demonstrated in [Ref-25], these alternative means of delivering the FSFs are not vulnerable to the original pipe whip or jet hazard.

7.6.3 Design Basis

7.6.3.1 Pipe Whip and Jet Impact Hazard Analysis Methodology

The pipe whip and jet impact hazard assessments have been performed based on the five steps below. This methodology is consistent with Section 7.2.1 and the further detail presented in section 7.3.2:

(1) Safety Classified SSCs and Class 1 divisional barriers are identified.
(2) The sources of potential pipe whip and jet impacts have been identified.
(3) Pipe whip and jet impact effects in rooms that contain both high energy pipework and SSCs that provide Fundamental Safety Functions have been characterised. This assessment included analysis of pipe whip path and jet shape, as well as forces and pressures.
(4) The consequences on SSCs that provide Fundamental Safety Functions, including Class 1 divisional barriers have been evaluated.
(5) Additional protection measures, if needed, are determined based on an evaluation of the impact on SSCs.

7.6.3.2 Assessment Assumptions

The following assumptions provide a basis for assessing postulated pipe whip and jet impact hazards:

- A pipe whip and jet impact can occur on the welds or heat affected zones of high energy pipework containing water or steam at a temperature greater than 95ºC and/or a pressure of greater than 1900 kPa (gauge).

- Only a single direct break potentially leading to a pipe whip/jet event take place at any given time, but secondary pipe break occurs as a direct result of an initial pipe whip and jet impact (i.e. the second event is not independent of the first.).
- Pipe whip and jet impacts may occur during normal operation, not during fault conditions (unless the fault causes a consequential pipe break).
- The combination of a pipe break and an independent fault is considered to be very low.

7.6.3.3 Design Requirement

The pipe whip and jet impact claim in Section 7.6.2 is achieved in the UK ABWR by the following:

- **Limiting the sources of pipe whip and jet impact** by reducing the amount of high energy pipework in the safety classified buildings.
- **Preventing pipe whip and jet impact hazard occurrence** through the design, manufacture and inspection of pipework in accordance with appropriate standards and reducing the number of weld locations in the high energy pipework.
- **Mitigating the consequences of severe pipe whip and jet impacts** by the use of pipe whip restraints where required.

7.6.3.4 Sources of Pipe Whip and Jet Impact Hazards

Pipe whip and jet impact are only assumed to occur in high energy pipework. NUREG 0800 is used as a guide to determine whether a pipe should be considered high energy and so to be the source of pipe whip or jet. Pipes that exceed these limits are considered to fail so as to potentially cause pipe whip and jet impact. Pipes marginally below this limit are considered on a case by case basis.

The main sources of high energy pipework in the UK ABWR are:

- Main Steam System (MS)
- Feedwater System (FDW)
- Heating Steam System (HS)
- Heating Steam and Condensate Water Return System (HSCR)
- Residual Heat Removal System (RHR)
- High Pressure Core Flooder System (HPCF)
- Reactor Core Isolation Cooling System (RCIC)
- Reactor Water Clean-up System (CUW)
- Control Rod Drive (System) (CRD)
- Standby Liquid Control System (SLC)

For high energy pipework that is included in the pipe whip and jet impact assessment, the locations of the postulated breaks are the terminal ends and intermediate locations where stress exceeds the thresholds according to ANSI/ANS 58.2-1988. In addition, intermediate welded locations are considered to identify whether more severe pipe whip and jet impact effects may occur.

7.6.3.5 Pipe Whip and Jet Impact Prevention and Protection

UK ABWR includes a number of design features that prevent pipe whip and jet impact:

- The number of welds in high energy pipework is minimized.
- Pipe stress analysis and pipe run optimisation is used to ensure that, wherever possible, piping is subject to low stress combinations.
- UK Class 1 high energy pipework is designed according to ASME Section III standards, including welds.
- The materials specified for the UK Class 1 high energy pipework systems are in accordance with ASME Section II.
- Inspection and testing of the UK Class 1 high energy pipework systems are in accordance with ASME Section V.
- Maintenance of UK Class 1 high energy pipework is in accordance with ASME Section XI.

High energy large bore pipework which potentially cause pipe whip and jet impact near the RPV includes pipe whip restraints to reduce the range of pipe whip and jet impact consequence.

7.6.3.6 Combined Hazards

As defined in section 7.3.2.2 and as assessed in Section 7.16, pipe whip and jets can be a cause of other correlated Internal Hazards. It is noted that the correlated combined events would only happen within the same division due to the divisional segregation provided in the UK ABWR design. In the case of a pipe whip and jet causing internal flooding, the internal flooding assessment (Section 7.5) has evaluated the impact of the internal flooding.

7.6.3.7 Pipe Whip and jet Impact Mitigation

If the pipe whip and jet impact prevention approaches described above are shown to be insufficient, additional measures may be implemented including modification of pipe routes, strengthening of barriers and/ or pipe whip restraints will be used to reduce the loads to acceptable levels.

7.6.4 Safety Evaluation

7.6.4.1 General Approach to Pipe Whip and Jet Impact Consequences

The UK ABWR is designed to prevent a pipe whip and jet impact from occurring. However, should this occur, failure of all equipment within the Class 1 division is assumed conservatively. Redundant equipment to maintain the Fundamental Safety Functions are provided in other Class 1 divisional areas, and this is protected from the effects of pipe whip and jet impact by appropriately designed Class 1 divisional barriers.

The Pipe whip and jet impact hazard assessment evaluates the impact and jet forces on walls and barriers (in particular Class 1 divisional barriers) to demonstrate that the barriers provide sufficient

separation to support this requirement for redundancy of SSCs required to deliver the Fundamental Safety Functions.

The analysis of the Class 1 barrier against pipe whip hazards is performed over a number of stages of increasing refinement as described in [Ref-4] and summarised below:

- An initial highly conservative assessment is used to eliminate those pipe whip scenarios that can easily be shown to satisfy the barrier acceptance criteria from further detailed consideration. If the initial assessment demonstrates that no perforation or scabbing occurs then the pipe whip scenario requires no further assessment.
- If the initial assessment identifies that scabbing is credible then a SSC review on the opposite side of the divisional barrier is performed to determine whether secondary hazards can occur or loss of safety significant SSCs in the adjacent division.
- If perforation is predicted in the initial assessment, or scabbing is predicted and cannot be accepted, then a two stage refined assessment of the pipe whip impact is performed.
- If the refined assessments still predict perforation or unacceptable scabbing, design modification options are considered.

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with Class 1 divisional barriers; in the case of the PCV, the MCR and the MSTR, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively. There are a limited number of additional cases where it is justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment, these exceptions to segregation have been assessed in [Ref-25], where it has been demonstrated that the FSFs can still be delivered and that the design is acceptable with respect to the pipe whip and jet impact hazards.

7.6.4.2 Consequences of pipe whip and jet impact

Section 5 of [Ref-34] presents the substantiation of the Class 1 divisional barriers against the potential jet loads when considered under the scabbing and perforation failure modes.

As discussed in Section 5 of [Ref-34], a large number of pipe whip scenarios are demonstrated to meet the perforation acceptance criteria using the initial screening criteria, and have required no further assessment to substantiate the barrier against the potential pipe whip loads when considered under the perforation failure modes. The perforation acceptance criterion is not met for a number of cases and the scabbing acceptance criteria is not met in the majority of cases.

A number of Class 1 barriers have required refined assessment as described in Section 7.6.4.1 above. These refined assessments have shown that, when more representative models are used, the Class 1 barriers are substantiated against the potential pipe whip loads when considered under the scabbing and perforation failure modes. There are a limited number of cases where the barrier thickness has been increased in response to other hazards and this has improved performance against scabbing and perforation.

During outages where hatches might be open, which may compromise the divisional segregation, the risk of a pipe whip or jet hazard is significantly lower than during at power modes (unlike for fire and explosion hazards) since most systems, except for the High Pressure Nitrogen Gas Supply System (HPIN) and Fire Protection System (FP), will either be discharged or will operate in the moderate energy region. A detailed assessment of pipe whip and jet impacts during outages is therefore not required.

7.6.5 ALARP Discussion

Sources of pipe whip and jet hazards have been minimised as far as is reasonably practicable by reducing the amount of high pressure pipework in the safety classified buildings and reducing the number of weld locations in the high pressure pipework.

In addition, the use of appropriate design standards for high pressure systems coupled with correct operation and EMIT represents relevant good practice and reduces the potential for pipe whip and jet hazards.

In all cases jet hazards are confined to the division of origin by the robust divisional barriers. The barriers have been demonstrated not to perforate following a Pipe whip hazard but, in a limited number of cases, scabbing of the barrier is accepted where it is demonstrated that the loss of any of the SSCs in rooms on the reverse side of the barrier would not result in a secondary hazard or jeopardise the delivery of the FSFs.

With respect to pipe whip and jet hazards, it is concluded that all reasonably practicable risk reduction measures have been implemented and that the residual risks are considered to be ALARP.

7.6.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of pipe whip and jet impacts, and prevent them from occurring. The design also provides for redundant and diverse equipment to maintain the FSFs in the case of such an Internal Hazard. This redundant and diverse equipment is protected by robust barriers and separation able to withstand jet impacts without scabbing or perforation. The barriers are also substantiated against the potential pipe whip loads when considered under the perforation failure mode. Scabbing of a small number of barriers as a result of pipe whip is accepted where the scabbing cannot compromise FSFs.

7.7 Dropped and Collapsed Loads

7.7.1 Introduction

The Topic Report on Dropped and Collapsed Loads [Ref-5] and the Topic Report on Dropped Loads Assessment of Nuclear Special Cranes [Ref-30] present the assessment of dropped and collapsed loads within the UK ABWR.

As discussed in [Ref-5], a dropped load is considered to be any item that can be dropped from a lifting device whereas a collapsed load is considered to be the collapse of a permanent SSC installed at height (e.g. collapse of lifting equipment) or collapse of a temporary structures, such as scaffolding, that may be installed during outage periods. The dropped or collapsed loads may cause damage to SSCs important to safety.

Nuclear Special Crane (NSC) dropped loads are defined in [Ref-30] as those loads associated with lifting operations undertaken on the Operating Deck (Room 705) with the Reactor Building Crane (RBC) and Fuel Handling Machine (FHM). Lifts and potential dropped loads related to the Spent Fuel Interim Storage (SFIS) are also considered. This hazard is only relevant to the R/B.

The possible consequences from a collapse of temporary structures cannot be assessed within the scope of the GDA, and will be addressed by a specific plant safety case assessment undertaken prior to the task being undertaken with the temporary structure required. This is because the consequence of collapsed loads could be bounded by that of dropped load and the specification of equipment required for detail assessment of collapsed loads will be determined during the post GDA phase.

Comprehensive Hazard Schedules, containing all bounding dropped load events identified, are presented within [Ref-5] and [Ref-30]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.7.2 Claims and Arguments

As for all other Internal Hazards, a principal objective of the internal dropped and collapsed load safety case is to limit the effects of any dropped load hazard to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5 and supported by the following safety claim specific to internal dropped loads.

Claim IH_D_SFC_5-7: General dropped load claim
Any dropped load event within the design basis will not prevent delivery of the Fundamental Safety Functions.

This and the general high level claims are then supported by lower level more detailed claims and arguments below and provide an auditable and logical process for demonstrating that the design intent has been achieved. These claims are derived by utilising experience, engineering judgment

and the safety philosophy/approach to hazards discussed in section 7.3.1, applied to the UK ABWR design. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH_D_SFC_5-7.1: Limiting dropped load to a single Class 1 division
The Class 1 divisional barriers segregating neighbouring divisions will be such that the consequences of design basis dropped/collapsed load events in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

(IH_D_SFC_5-7.1.A1 & IH_D_SFC_5-7.1.A2)
For buildings containing multiple redundant divisions of Class 1 equipment, the divisions are segregated by Class 1 divisional barriers of sufficient integrity that dropped loads are contained to the division where they originate (i.e. the dropped load does not perforate the barrier).

(IH_D_SFC_5-7.1.A3)
Any effects from an internal dropped load event in one division (e.g. concrete scabbing) will not initiate a hazard event in a different division, and will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

Section 7.7.4 presents the detailed assessment of the barrier responses to dropped loads and demonstrates that in all cases the barriers can be substantiated to safely absorb the dropped load impact energy.

7.7.3 Design Basis

7.7.3.1 Dropped Load Hazard Analysis Methodology

The Dropped Loads Hazard Assessment has been performed based on the following approach. This methodology is consistent with Section 7.2.1 and the further detail presented in section 7.3.2:

(1) Identification of the lift to be performed (including the lifting equipment and room of origin).
(2) Identify the SSCs in the room of origin and determine which division they belong to.
(3) Determine whether the dropped load has a potential to damage system or components of different Class 1 divisions.
(4) Identify the impact energy of the lifts that could not create damage even to the thinnest divisional barrier slab.
(5) Identify whether the room of origin and the room beneath are within same safety division.
(6) Determine whether the dropped load has sufficient Impact Energy to breach the room boundary, either through perforation or scabbing.
(7) Identify any modifications to room layout or dropped load protection that can be implemented to mitigate the consequences of a dropped load.

7.7.3.2 Assessment Assumptions

The following assumptions provide the basis for assessing dropped load hazards:

- A dropped load can result from any lifting device in service on the site, either permanent or temporary.
- A dropped/ collapsed load hazard may also occur due to collapse of a lifting device at height.
- A dropped/ collapsed load may occur at power or during outage.
- A dropped load may occur as a result of operator error as well as equipment failure, including failure of a high integrity lifting device.
- The potential for a secondary dropped/ collapsed load due to a prior dropped/ collapsed load is considered.
- A dropped/ collapsed load hazard may occur as a result of another internal/external event.
- Multiple dropped/ collapsed loads caused by a single event such as an earthquake may occur.
- No more than a single dropped load can occur at any one time in a defined damage range.

It is recognised that the majority of dropped loads are caused by slinging faults or other operator errors. The design of the lifting devices is a site specific issue but will be such as to minimise the potential for operator error. All lifting devices will be designed and supported to appropriate standards. Temporary construction elements will be embedded in the structure.

7.7.3.3 Design Requirement

The dropped and collapsed load claim in Section 7.7.2 has been achieved in the UK ABWR by to following:

- **Limiting the sources of dropped and collapsed loads**. The number of lifting operations is reduced as far as reasonably practicable, with each item generally only being required to be lifted once. Where lifting is necessary specific hoists designed for the equipment to be lifted are used.
- **Prevention of dropped and collapsed loads**. Installed lifting equipment are of a suitable design and sufficient capability to complete the lifts. Where possible lifting operations are avoided completely. Suitably qualified permanent structures, pipe and equipment supports and access platforms are used.
- **Optimisation of equipment lifting routes**. Lifting routes are chosen that minimise the requirement for equipment to transfer over potentially vulnerable SSCs. Wherever possible lifting routes do not interact with each other.
- **Mitigating the consequences of severe dropped and collapsed loads**. Where lifting routes cannot avoid vulnerable equipment or lifting heights are necessarily high, then impact protection is used.

7.7.3.4 Sources of Dropped and Collapsed Load Hazards

The main sources of potential dropped loads in the UK ABWR are as follows:

- R/B overhead crane
- Fuel Handling Machine (FHM)

- R/B maintenance area cranes
- Crane in the Hoist Well
- Jib crane in the Hoist Well
- T/B Operating Deck cranes
- Rw/B cranes
- Monorails and chain blocks used to perform lifting operations in equipment areas.

These cranes and lifting devices could also be sources of collapsed loads if the cranes or monorails were to fail with or without a load. There are also a variety of support structures installed during construction that will be left in place after construction is complete.

7.7.3.5 Dropped and Collapsed Load Prevention and Protection

The UK ABWR includes a number of design features that prevent dropped loads, as described below:

- Lifting devices are designed using the appropriate design codes. Engineered lifting beams are used for many heavy lifts to minimise potential for errors in slinging arrangements (e.g. RPV head, dryer module).
- The R/B crane and fuel handling machine have redundant load paths to prevent a single failure leading to a dropped load.
- The R/B crane and fuel handling machine have latched hooks to prevent slipping faults.
- The R/B crane and fuel handling machine have an electromagnetic brake system to prevent dropped loads in the event of hoist failure.
- Monorails are provided for maintenance of heavy equipment and equipment is designed with engineered lifting points where possible.
- Design of equipment, interlocks, operational procedures and operator training restrict operators from lifting loads beyond the capability of the lifting device.
- Interlocks are provided to restrict movement of cranes for safety critical lifts.

The FHM and the R/B overhead crane are the only Class 1 lifting devices and specific details, including the interlocks and other dropped load prevention devices, can be found in Sections 19.6 (Fuel Handling Machine Related System) and 19.7 (Reactor Building Overhead Crane) of PCSR Chapter 19: Fuel Storage and Handling.

The hazards from a dropped load are significantly reduced by restricting certain lifting operations to outages. Some lifting devices are operated only for maintenance of equipment and therefore any dropped loads will not affect equipment other than that under maintenance. Lifting devices operating in areas with equipment important to safety (except R/B crane and fuel handling machine) is assumed to remove that division from service. As the divisions are segregated by appropriately rated Class 1 divisional barriers, the other Divisions are available even in the event of a dropped load in the affected Division.

The R/B crane is designed to take into account the heaviest loads in the R/B (reactor well plug, reactor head, dryer, separator, spent fuel cask). A load cell in the R/B crane prevents the crane from operating if the load is greater than the crane rating (e.g. if there is a snagged load). The R/B overhead crane has a number of operating modes with interlocks to limit the area over which it can operate. An example is that the R/B crane will be prevented from handling any heavy loads over the spent fuel racks and from handling a spent fuel cask over the spent fuel racks or reactor well by interlocks.

The fuel handling machine has similar interlocks to limit operational area when handling fuel assemblies and also has vertical position interlocks to ensure sufficient water shielding over the spent fuel being handled.

The R/B crane and FHM are designed to prevent a dropped load (e.g. redundant load paths) and allow recovery (e.g. manual gearbox drives to enable recovery of load following failure of lifting device hoisting mechanisms).

There is a process for the layout designers and the system designers to review the overall design to ensure dropped loads do not impact important equipment, pipework, ducts and cables, by layout of equipment and, where necessary, identification of defined load paths.

7.7.3.6 Combined Hazards

As per the definition in section 7.3.2.2 and as assessed in Section 7.16, a dropped load can be a cause of other consequential Internal Hazards. It is noted that consequential combined events would generally only occur within the same division due to the divisional segregation provided in the UK ABWR design.

7.7.3.7 Dropped and Collapsed Load Mitigation

If all the dropped load prevention approaches described above were to fail, the general approach to ensuring protection of SSCs of the Fundamental Safety Functions is to limit the impacts of a dropped load to within the affected Division. The dropped load claim is achieved by mitigating the consequences as described in section 7.3.1.8 and demonstrating that there are no significant residual risks.

7.7.4 Safety Evaluation

The identification of potential dropped loads in [Ref-5] and [Ref-30] has shown that the only buildings in which a dropped load assessment is required is the R/B, Hx/B and C/B. All other buildings can be screened out either on the basis that there is only a single A-1 division within the building (for example the EDG/Bs) or there are no safety classified equipment which contribute to the delivery of the Fundamental Safety Functions.

The dropped load hazard assessment assumes that all SSCs in a room in which a dropped load occurs are lost due to the dropped load (this in turn is pessimistically assumed to lead to the loss of

the associated Class 1 division). In addition, the dropped load hazard assessment has included estimates of the impacts created from the dropped load. The impact estimates have been used to determine appropriate civil and structural design, where necessary.

To simplify the assessment, a threshold value was determined in [Ref-5] for the impact energy that can be withstood by the thinnest floor slab without failure. The potential dropped loads were then reviewed in [Ref-5] and those with impact energies smaller than this bounding scenario are screened from further assessment. For dropped loads with impact energies larger than the bounding case, separate detailed assessments of the impact load on the specific barriers affected was carried out.

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with structural barriers; in the case of the PCV, the MCR and the MSTR, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively. There are a limited number of additional cases where it is justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment, these exceptions to segregation have been assessed in [Ref-25], where it has been demonstrated that the FSFs can still be delivered and that the design is acceptable with respect to the dropped load hazard.

7.7.4.1 Consequences of dropped loads in the R/B

There are 66 potential dropped loads identified in R/B include the NSC loads discussed below, the loads in the PCV and MSTR discussed in the other chapter. 6 items are identified in [Ref-5] as exceeding the threshold value for detailed analysis.

Following this detailed analysis, there are no cases identified where perforation may occur. Therefore, the consequences of dropped loads in the R/B will be contained within the safety division of origin and will not cause risk to nuclear safety.

7.7.4.2 Consequences of dropped NSC loads in the R/B

The dropped loads for NSCs are considered and the assessment of the dropped load consequences using R3 in [Ref-30]. It was determined that a NSC dropped load does not have compromise SSCs which provide nuclear safety, however, the drop of Reactor Well Shield Plug onto the operating deck has a potential to result in perforation. A scoping assessment has been undertaken to consider the overall structural response, or global response, of the Operating Deck structure under impact from a dropped section of the Reactor Well Shield Plug [Ref-34]. The scoping assessment has demonstrated that with an increase in slab thickness, increase in shear reinforcement at the supports and the optimisation of bending reinforcement proposed above, there is a high degree of confidence that the Operating Deck structure responds in a controlled, ductile mode under impact loading and can safely absorb the dropped load impact energy.

7.7.4.3 Consequences of dropped loads in the Hx/B

There are 27 potential dropped loads identified in Hx/B [Ref-5].

Only one lifting operation within the Heat Exchanger Building occurs above rooms belonging to a different Safety Division, and exceeds the threshold value for detailed analysis. This detailed analysis indicates that scabbing of the divisional barrier (floor slab) may occur. As a mitigation against scabbing causing a secondary impact on SSCs of another division, the floor slab will be reinforced to ensure that scabbing does not occur [Ref-34].

7.7.4.4 Consequences of dropped loads in the C/B

There are 27 potential dropped loads identified in C/B [Ref-5]

Only one lifting operation within the Control Building occurs above rooms belonging to a different Safety Division, and exceeds the threshold value for detailed analysis. This detailed analysis indicates that scabbing of the divisional barrier (floor slab) may occur. As a mitigation against scabbing causing a secondary impact on SSCs of another division, the floor slab will be reinforced to ensure that scabbing does not occur [Ref-34].

7.7.5 ALARP Discussion

The number of lifting operations is reduced as far as reasonably practicable, with each item generally only being required to be lifted once. Installed lifting equipment is designed using relevant standards and has sufficient capability to complete the lifts. Consistent with relevant good practice, lifting routes are chosen that minimise the requirement for equipment to transfer over potentially vulnerable SSCs. Wherever possible lifting routes do not interact with each other.

7.7.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of dropped and collapsed loads, and prevent them from occurring. The design also provides for redundant and diverse equipment to maintain the Fundamental Safety Functions in the case of a dropped or collapsed load. This redundant and diverse equipment is protected by separation and by robust Class 1 divisional barriers able to withstand the dropped and collapsed loads. The Dropped Load Hazard Assessment completed during GDA Step 4 has demonstrated that the UK ABWR is designed so that any dropped load event within the design basis will not compromise the Fundamental Safety Functions.

7.8 Internal Missiles

7.8.1 Introduction

The Topic Report on Internal Missile – Conventional Internal Missiles [Ref-6] presents the assessment of conventional internal missiles within the UK ABWR.

Conventional Internal missiles sources are defined as pressurised components (e.g. a pressure vessel) and rotating machinery (e.g. turbine-generators, diesel generators, pumps, fans, blowers, compressors, etc.) that can fail disruptively. Internal missiles may be generated when a vessel disintegrates or in the event of the failure of rotating machinery.

Due to the exceptional nature of the main steam turbine missile, for the purposes of the internal missiles assessment the two categories of internal missiles are considered separately. This Section considers all internal missiles other than those generated as a result of Main Turbine Disintegration, whilst Section 7.15 considers Main Turbine Disintegration.

A comprehensive Hazard Schedule, containing all bounding conventional missile events identified, is presented within [Ref-6]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.8.2 Claims and Arguments

As for all other Internal Hazards, a principal objective of the internal missile safety case is to limit the effects of any internal missile hazard to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5 and supported by the following hazard specific safety claim.

Claim IH CM SFC 5-7.1: Conventional Internal Missile Claim
An Internal Missile event within the design basis will not prevent delivery of the Fundamental Safety Functions.

This high level claim is then supported by the lower level more detailed claims and arguments below which combined, demonstrate the higher level claim. These claims are derived by utilising experience, engineering judgment and the safety philosophy/approach to hazards discussed in section 7.3.1, applied to the UK ABWR design. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH CM SFC 5-7.1.1: Rotating equipment is only operated with the designed casing in place.

(IH CM SFC 5-7.1.1.A1)
In determining whether or not rotating equipment presents a design basis missile source, the performance of the “as designed casings” is taken into consideration. In cases where the missile

energy is less than the impact withstand of the casing, the missile can be discounted (see Step 3 of the Internal Missile Hazard Analysis Methodology in Section 7.8.3.1. This leads to a claim on the operation of rotating equipment only with the "as designed" casings in place.

Claim IH CM SFC 5-7.2: The Class 1 divisional barriers segregating neighbouring divisions will be such that the consequences of a design basis internal missile event in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

(IH CM SFC 5-7.2.A1 & IH CM SFC 5-7.2.A2)
For buildings containing multiple redundant divisions of Class 1 equipment, the divisions are segregated by Class 1 divisional barriers of sufficient integrity that conventional missiles are contained to the division in which they originate (i.e. the missile does not perforate the barrier).

(IH CM SFC 5-7.2.A3)
Any effects from an internal missile event in one division (e.g. concrete scabbing) will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

Section 7.8.4 presents the detailed assessment of the barrier responses to conventional missiles and demonstrates that the barriers can be substantiated to safely absorb the missile impact energy.

7.8.3 Design Basis

7.8.3.1 Internal Missile Hazard Analysis Methodology

The internal missile hazard analysis has been performed based on the following approach. This methodology is consistent with Section 7.2.1 and the further detail presented in section 7.3.2:

(1) Definition of the area considered. This is a top down process in which the assessment is divided into Rooms or areas to be considered. These areas defined so as to provide a boundary for the assessment.
(2) Identification of potential sources of internal missile. Each Room or area is considered in turn to identify sources of missiles including :
    (a) High energy pipework (e.g. steam or water pipes).
    (b) Elements on high energy pipework (specifically valve stems).
    (c) High pressure equipment.
    (d) Rotating equipment (pumps, fans, generators and compressors).
(3) For rotating equipment assess the impact withstand of equipment casing:
    (a) If the casing withstand is greater than the translational energy of the potential missile then the source can be discounted from the assessment.
    (b) If the casing withstand is less than the translational energy of the potential missile then the assessment steps below apply.
(4) Identification of SSCs required to deliver the Fundamental Safety Functions. Safety classified SSCs in each of the Rooms/ areas are identified, in addition safety classified SSCs in adjacent Rooms/ areas are identified. The Class 1 divisions that the SSCs relate to are determined.

(5) Assessment of internal missile consequences. The characteristics of the potential internal missile are determined; its translational energy calculated, the barrier response determined and consequential damage to SSCs in adjacent Rooms/ areas determined in case of potential scabbing or perforation.
(6) Assessment of internal missile frequencies. Should an internal missile result in unacceptable consequences (i.e. affecting multiple Class 1 divisions), then the frequency is assessed to determine whether the internal missile event is low frequency or beyond design basis.
(7) ALARP assessment.

7.8.3.2 Assessment Assumptions

The following assumptions provide the basis for assessing postulated missile hazards:

- A missile can occur anywhere on the site where permanent or transient missile sources are located.
- Only a single missile event takes place at any given time, except where secondary missiles are induced as a direct result of an initial missile (i.e. the secondary missile is a consequence of the primary).
- Missile hazards may occur during all operating modes.
- A missile may be induced as a result of another internal/external event.
- Pipework is not considered as a missile source due to the high ductility, it is considered as a Pipe Whip hazard and is assessed in Section 7.6 above.
- The weak point of a pipework structure is the pipework itself and not the valves; therefore, it is assumed that the pipework fails first. The resulting pressure loss would not result in a valve missile. More generally, elements on high energy piping (flanged and other bolted elements, valves stem and bonnets, valve bodies) are excluded as a source of missiles.
- Missiles are assumed only to lose energy through their interaction with the divisional barriers (walls, floors and ceilings of the room) and not through any other structures within the originating Room or area.

7.8.3.3 Design Requirement

The internal missiles claim in Section 7.8.2 has been achieved in the UK ABWR by:

- **Limiting the sources of internal missiles** by reducing the number of pressure systems and rotating equipment where possible.
- **Prevention of internal missile generation** through design and manufacturing according to appropriate international design and operational health and safety standards.
- **Optimising the orientation of equipment and layout of areas** such that the number of SSCs at risk is minimised.
- **Mitigating the consequences of internal missiles** through the use of suitable barriers.

7.8.3.4 Sources of Internal Missiles

Potential sources of internal missile include:

- High energy equipment,
- Pumps,
- Fans,
- Generators, and
- Compressors.

7.8.3.5 Prevention of Internal Missile Generation

UK ABWR includes a number of design features that prevent a missile:

- Equipment is designed and manufactured according to appropriate international design and operational health and safety standards (See Section 5.8 of this PCSR Chapter 5 : Applied Regulations, Codes and Standards).
- Appropriate quality assurance programs are followed in design and fabrication of the equipment and any casings.
- Commissioning, testing and inspection of equipment ensure equipment performs and continues to perform as intended.
- Overspeed detection and trip systems against overspeed of rotating machinery are installed where required.
- Detection and relief systems for over-pressure in tanks and vessels are installed in accordance with appropriate UK regulations (e.g. Pressure Systems Safety Regulations) where required.

7.8.3.6 Combined Hazards

As per the definition in section 7.3.2.2 and as assessed in Section 7.16, internal missiles can be a cause of other Internal Hazards, including secondary missiles, pipe whip, and flooding.

7.8.3.7 Mitigating the Consequences of Internal Missiles

Rotating equipment is fitted with casings that attenuate the energy of any missiles generated through equipment failure.

If all the missile prevention measures described above were to fail, the general approach is to limit the impacts of the missile to within the affected Division. In some areas, it is necessary to consider secondary missiles (e.g. scabbing concrete) due to the proximity of the hazards. In these cases, consequences are assessed and other protection and mitigation measures are considered if necessary.

7.8.4 Safety Evaluation

7.8.4.1 General Approach to Internal Missile Consequences

The internal missile hazard analysis pessimistically assumes that a missile will result in the loss of all equipment in a division where the missile originates. In addition it assesses the divisional barrier

walls, ceilings and floors to determine whether divisional segregation is compromised by the missile and equipment in other divisions is also compromised.

The identification of potential conventional missiles in [Ref-6] has shown that the only buildings in which a conventional missile assessment is required is the R/B, the C/B and the T/B. All other buildings can be screened out either on the basis that there is only a single A-1 division within the building or there are no safety classified equipment which contribute to the delivery of the Fundamental Safety Functions. Whilst a conventional missile hazard event in one of the EDG/B's will still leave two sets of redundant SSCs in the other EDG/Bs available to deliver the FSFs, the EDG/B building itself could be a potential missile source for other buildings and therefore an assessment of a conventional missile originating from the EDG/Bs has been performed.

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with barriers; in the case of the PCV, the MCR and the MSTR, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively. There are a limited number of additional cases where it is justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment, these exceptions to segregation have been assessed in [Ref-25], where it has been demonstrated that the FSFs can still be delivered and that the design is acceptable with respect to the internal missile hazard.

7.8.4.2 Consequences of internal missiles

An assessment of the identified missile sources within the R/B has identified that a small number of conventional missiles could initially perforate a divisional barrier [Ref-6]. These identified barriers have been strengthened to prevent perforation from occuring (Section 8 of [Ref-34]). In addition, scabbing is credible for a number of barriers within the R/B, however a detailed assessment of the SSCs in the adjacent rooms has shown that this scabbing cannot lead to failure of SSCs that deliver the FSFs. Therefore these limited scabbing cases are considered acceptable in demonstrating the conventional missile claims detailed in Section 7.8.2 above.

An assessment of the identified missile sources within the C/B has shown that the majority of the conventional missiles from rotating equipment are retained in their casing [Ref-6]. Similar to the R/B, scabbing is credible for a small number of barriers within the C/B, however a detailed assessment of the adjacent rooms has shown that this cannot lead to failure of SSCs that deliver the FSFs.

The largest conventional missile source in the UK ABWR is located on the ground floor of the C/B. Assessment of this missile has shown that perforation of a number of barriers could occur. Other areas on the ground floor of the C/B contain no SSCs so perforation of the barriers on this floor is acceptable. However neither perforation nor scabbing of the slab above the missile source is acceptable and the slab has been thickened so that there is no credible risk of scabbing in the above rooms which contain SSCs (Section 8 of [Ref-34]).

An assessment of the identified missile sources within the T/B has shown using engineering judgement that the potential missile sources are sufficiently separated by a number of robust

structures from the MSTR, the A-1 SSCs contained in the C/B adjacent to the T/B as well as OG sensitive SSCs so that the missile consequences will not prevent the delivery of the FSFs or cause any consequent radioactive releases.

An assessment of the conventional missile originating inside of an EDG/B building has shown that the missile has the potential to perforate the external wall of its own building and potentially cause scabbing to the weakest external wall of a different building containing safety related SSCs [Ref-6]. The reinforcement amount in the exterior walls of the EDG/B will be increased to ensure that scabbing to the thinnest structure of any other building containing class 1 SSCs cannot occur and the FSFs continue to be delivered (Section 8 of [Ref-34]).

7.8.5 ALARP Discussion

Sources of conventional missile hazards have been minimised as far as is reasonably practicable by reducing the number of pressure systems and rotating equipment in the safety classified buildings. In addition, the use of appropriate design standards for high pressure systems and rotating equipment coupled with correct operation, EMIT and inclusion of safety features such as pressure release valves and overspeed detection and trip systems represents relevant good practice and reduces the potential for conventional missile hazards.

A small number of conventional missiles have impact energies that could result in perforation or scabbing of the opposite face of the barrier with an associated secondary hazard. In each instance, modification to the reinforcement of the barrier has been identified that will ensure that the divisional barrier resists the required impact loading.

7.8.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of internal missiles and prevent them from occurring. In the case of rotating equipment, account has been taken of the impact withstand of the casing in determining the energy of missile sources. In some cases, this has led to the removal of the missile as a source for assessment.

The design also provides for redundant and diverse equipment to maintain the Fundamental Safety Functions in the case of such an Internal Hazard. This redundant and diverse equipment is protected by separation and robust Class 1 divisional barriers able to withstand the missile impacts. The internal missile assessment demonstrates that the UK ABWR is designed so that any missile impact (from sources other than the Main Turbine discussed in Section 7.15) within the design basis will not compromise delivery of the Fundamental Safety Functions.

7.9 Internal Blast

7.9.1 Introduction

The Topic Report on Internal Blast [Ref-7] considers non-combustible explosions following the sudden release of energy from a pressurised vessel, pipe or component. Blast hazards are assessed separately to explosions of combustible material and HEAF (see Section 7.4), and other pressurised component failure modes such as pipe whip (see Section 7.6) and missile (see Section 7.8). All pressurised vessels, components and piping are assessed, regardless of the nature of the liquid or gas that would be released if they did fail.

The sudden release of energy during an internal blast generates a shockwave with the potential to damage components or structures. Any missiles generated as part of the internal blast are assessed separately as internal missiles in Section 7.8.

A comprehensive Hazard Schedule, containing all bounding blast hazard events identified, is presented within the Topic Report on Internal Blast [Ref-7]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.9.2 Claims and Arguments

As for all other Internal Hazards, a principal objective of the internal blast safety case is to limit the effects of any blast hazard to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5. Appendix A presents the full claims table for this PCSR Chapter; no hazard specific claims are required for blast, however the following hazard specific arguments have been developed in support of claims IH SFC 5-7.2 and IH SFC 5-7.3:

(IH B SFC 5-7.1.A1 & IH B SFC 5-7.1.A2)
For buildings containing multiple redundant divisions of Class 1 equipment, the divisions are segregated by Class 1 divisional barriers of sufficient integrity that blasts are contained within the division where they originate (i.e. the blast does not perforate or scab the barrier). This is demonstrated within [Ref-7], where all identified blast hazards are contained by the Class 1 divisional barriers. Blast sources have been identified within the R/B and C/B, whilst no sources have been identified in the Hx/B.

(IH B SFC 5-7.1.A3)
Where there are penetrations or open doors in rooms, the effects of a non-combustible blast can propagate into the surrounding rooms. However, blast modelling has shown that the energy dissipates to a level that would be deemed non-hazardous as the shockwave travels through a penetration between divisions and A-1 SSCs from different safety divisions will not be affected [Ref-40].

(IH B SFC 5-7.1.A4)
A number of blast sources have been identified in the T/B, detailed blast modelling has shown that no sources have sufficient energy to damage systems containing radioactive materials or A-1 SSCs contained in areas adjacent to the T/B (MSTR and C/B) [Ref-40].

(IH B SFC 5-7.1.A5, IH B SFC 5-7.1.A6 & IH B SFC 5-7.1.A7)
Blast modelling [Ref-40] has shown that a blast in the B/B does not propagate from the room of origin and does not lead to a loss of A-1 SSCs. Similarly, a blast in an EDG/B may lead to a loss of the EDG but has been demonstrated not to propagate outside of the building and there is no effect on the redundant EDGs.

No blast sources exceeding the threshold for analysis, determined in [Ref-40] and described in Section 7.9.4.1 below, have been identified within the remaining buildings within the scope of the GDA.

(IH B SFC 5-7.3.A1 & IH B SFC 5-7.3.A2)
Exception to Segregation SSCs vulnerable to failure from blast are, where possible, designed to fail safe. In addition alternative means of delivering the FSFs exist for all exception to segregation SSCs. As demonstrated in [Ref-25], these alternative means of delivering the FSFs are not vulnerable to the original blast hazard.

7.9.3 Design Basis

7.9.3.1 Blast Hazard Analysis Methodology

The blast hazard assessment has been performed based on the following approach. This methodology is consistent with section 7.2.1 and the further detail presented in section 7.3.2:

1. The identification of A-1 classified SSCs for all the buildings inside the nuclear island, on a room by room basis.
2. Identification of all the non-combustible blast hazards for each area/building of the UK ABWR.
3. Characterization of the blast hazards and determination of the equivalent blast energy in TNT equivalent mass is determined for onerous non-combustible blast hazards.
4. Identify the safety measures in place to deal with a non-combustible internal blast event, and demonstrate that the effects of an internal blast event is limited to a single division.

7.9.3.2 Assessment Assumptions

The following assumptions are made for the internal blast assessment:

1. An internal blast may occur at any high energy compartment/area which contains permanent or transient pressurised systems.
2. An internal blast may occur from any high energy component during normal operation or shutdown.

3. An internal blast may occur as a result of another internal/external event.
4. A single internal blast may occur at any time as a result of an independent event.
5. Multiple internal blasts may occur as a result of a single event such as an earthquake. Appropriate provisions will be developed.

7.9.3.3 Design Requirement

The general Internal Hazard Claims in Section 7.9.2 will be achieved in the UK ABWR by:

1. **Limiting the sources of blast** as much as possible by reducing the number of pressurised vessels and the amount of high pressure pipework in the safety classified buildings and reducing the number of weld locations in the high pressure pipework.
2. **Preventing blast hazard occurrence** through correct operation of pressurised systems, EMIT and inclusion of safety features such as pressure release valves.
3. **Mitigating the consequences of severe blasts**, principally using reinforced concrete barriers.

7.9.3.4 Sources of Blast Hazards

Identification of internal non-combustible blast hazards has been undertaken systematically for each building and area within the UK ABWR. The types of non-combustible internal blast hazards considered are:

- High pressure vessels
- High pressure gas (non-steam) piping
- High pressure water piping
- High pressure steam piping

The term “high pressure” refers to any component with pressure above 1.9MPa. To increase the level of conservatism, all the piping above ambient pressure have been considered for the purpose of the assessment. This also eliminated the ‘cliff edge’ effect, where the assessed component has pressure below 1.9MPa, but may present significant blast hazards due to other factors.

Although in practice high pressure components within the UK ABWR are designed to fail in a ductile manner, however all pressure vessels within the UK ABWR are assumed to fail in a brittle manner following an unspecified failure. Assuming brittle failure means no blast energy is dissipated during the rupturing of the vessel. It is also assumed that all energy within the vessel is released instantaneously. The most onerous piping failure modes have been assumed, providing margin in the assessment.

The main sources of potential high pressure pipework in the buildings containing SSCs important to safety within the UK ABWR are:

- Main Steam System (MS).
- Main Feedwater System (FDW).

- Residual Heat Removal System (RHR).
- High Pressure Core Flooder System (HPCF).
- Reactor Core Isolation Cooling System (RCIC).
- Reactor Water Cleanup System (CUW).
- Control Rod Drive system (CRD).
- Standby Liquid Control system (SLC).
- Hydraulic Control Unit (HCU).

7.9.3.5 Prevention of Blast Hazards

UK ABWR includes a number of design features that prevent blast:

- Equipment is designed and manufactured according to appropriate international design and operational health and safety standards (See Section 5.8 of PCSR Chapter 5 : Applied Regulations, Codes and Standards).
- Appropriate quality assurance programs are followed in design and fabrication.
- Commissioning, testing and inspection of equipment ensures equipment performs and continues to perform as intended.
- Detection and relief systems for over-pressure in tanks and vessels.

Additionally, where possible, potential sources of blast will be kept away from sensitive equipment and from the divisional and non-divisional barriers that protect redundant safety equipment.

7.9.3.6 Combined Hazards

As per the definition in section 7.3.2.2 and as assessed in Section 7.16, internal blast can be a cause of other Internal Hazards. It is noted that consequential combined events would only happen within the same division due to the divisional segregation provided in the UK ABWR design.

7.9.3.7 Mitigating the Consequences of Blast

In the unlikely event where the design, correct operation and maintenance of high energy pipes and vessels do not prevent their failure, a blast wave may result. As demonstrated through the detailed blast modelling [Ref-40] and barrier substantiation [Ref-34], the UK ABWR is designed with robust, reinforced concrete barriers that can withstand the effects of any blast that could occur across the plant, thus limiting the damage to a single division of the primary (A-1 SSCs) safety systems or the backup safety systems (A-2 SSCs).

In fact, the blast effects are likely in many cases to be greatly mitigated before reaching a Class 1 barrier as account has not been taken for any internal walls or other obstructions that would dissipate the blast wave's energy.

7.9.4 Safety Evaluation

7.9.4.1 General Approach to Blast Consequences

Where blasts are assumed to occur, although in most cases there would be only local damage, it is pessimistically assumed that all SSCs in the division of origin are lost during the hazard.

To simplify the assessment, a conservative value was calculated in the Internal Blast Modelling Report [Ref-40] for the largest blast load that can be withstood by the thinnest wall (divisional barrier or otherwise) without failure in rotation or shear. The potential sources of internal blast were then reviewed in [Ref-7] to confirm that blast loads would be smaller than this bounding scenario. For blast sources whose load is potentially larger than the bounding case, separate detailed assessments of the blast load on the affected barriers was carried out.

Where they exist in Class 1 divisional or non-divisional barriers, penetrations for e.g. HVAC or doors might allow blast effects to spread to compartments containing redundant, primary safety systems of another division. However, modelling in [Ref-40] demonstrates that even the most onerous blast sources may only cause damage to SSCs on the far side of the barrier if the blast source is close to the penetration. Therefore, potential blast sources are located away from penetrations through Class 1 divisional or non-divisional barriers wherever possible. Consequently, open doors or hatches in barriers during outage operations are not expected to compromise the ability to deliver the FSFs as demonstrated in [Ref-40].

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with barriers; in the case of the PCV, the MCR and the MSTR, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively. There are a limited number of additional cases where it is justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment, these exceptions to segregation have been assessed in [Ref-25], where it has been demonstrated that the FSFs can still be delivered and that the design is acceptable with respect to the internal blast hazard.

7.9.4.2 Consequences of an internal blast

The R/B contains the majority of high pressure systems within the UK ABWR. The TR on Internal Blast [Ref-7] shows that the magnitude of the internal blast hazards presented within the R/B do not exceed the blast load capacity for this ‘weakest barrier’ bounding scenario. Therefore, all Class 1 Barriers within the R/B are demonstrated to withstand blast hazards (i.e. no perforation or scabbing). It should be noted that a blast originating within the MSTR is not assessed in [Ref-12] and has been subject to a separate analysis as summarised in Section 7.14.

The C/B has only a small number of non-combustible blast hazards in comparison to the R/B. All of these non-combustible blast hazards are in the form of high pressure piping, ranging from small bore pipes to large bore main steam piping. [Ref-7] shows that this high pressure piping generates blast loads significantly lower than the bounding scenario. Therefore, all Class 1 Barriers within the C/B are demonstrated to withstand blast hazards (i.e. no perforation or scabbing).

The magnitude of the potential non-combustible blast hazards are higher in the T/B than in the R/B and C/B and have the potential to produce a blast larger than the bounding scenario [Ref-7]. Detailed modelling in [Ref-40] demonstrates that the non-divisional compartment barriers within the T/B are fully substantiated against the blast hazard and there is no propagation of blast hazards outside of the room of origin. There are exception to segregation SSCs identified within the T/B which are assumed to fail as a result of the blast. These are sensors split into groups of four with each group comprised of a sensor associated with each of the four electrical divisions. The sensors are configured as 'fail safe' and therefore loss of multiple sensors across the divisions will not result in a loss of the Fundamental Safety Functions.

The B/B and EDG/B each have only a small number of non-combustible blast hazards [Ref-7]. In both buildings the Starting Air Receiver Tanks have the potential to produce a blast larger than the bounding scenario and have been subject to detailed assessment. All other blast sources are below the load capacity of the bounding scenario.

Detailed blast modelling in [Ref-40] has shown that the blast effects are contained with the room of origin. The B/B contains no A-1 SSCs but does contain A-2 support systems, however the assessment has shown that there are no blast sources with the potential to damage any such systems. Whilst the EDG is assumed to have failed in the blast, there is no propagation of the hazard outside the building of origin and the redundant EDGs remain available to deliver the FSFs.

7.9.5 ALARP Discussion

Sources of blast hazards have been minimised as far as is reasonably practicable by reducing the number of pressurised vessels and the amount of high pressure pipework in the safety classified buildings and reducing the number of weld locations in the high pressure pipework. In addition, the use of appropriate design standards for high pressure systems coupled with correct operation, EMIT and inclusion of safety features such as pressure release valves represents relevant good practice and reduces the potential for blast hazards.

Throughout the R/B and C/B the internal non-combustible blast consequences are limited to the room or compartment where the non-combustible blast event occurs by the robust divisional barriers. For the T/B, where there are no divisional safety barriers, it has been demonstrated that the internal non-combustible blast consequences do not cause damage to any critical A-1 SSCs (due to fail safe nature of instrumentation) or OG SSCs containing radioactive materials. For the B/B and EDG/B blast effects are limited to the room of origin, and there is suitable redundancy of systems to ensure that the FSFs continue to be delivered.

It is concluded that the UK ABWR design generally meets relevant good practice to either prevent blast sources or effectively mitigate their consequences such that risks are ALARP.

7.9.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of blast and prevent them from occurring. The design also provides for redundant and diverse equipment to maintain the Fundamental Safety Functions in the case of such an Internal Hazard. This redundant and diverse equipment is protected by robust Class 1 divisional barriers that are capable of resisting any potential blast effects. The blast assessment demonstrates that any blast event within the design basis will not compromise the Fundamental Safety Functions.

7.10 EMI/RFI

7.10.1 Introduction

The sources of EMI/RFI can be categorised as natural and man-made sources. There are two main types of emission: conducted emission and radiated emission. The conducted emission is the noise transmitted within cables, and the radiated emission is radio frequency noise radiated to the general environment. Hereinafter we refer to both conducted emission and radiated emission as EMI/RFI.

EMI/RFI is potentially capable of disabling sensitive electronic equipment or causing spurious activation of equipment which may have nuclear safety related functions.

The principal means of protection from the EMI/RFI hazard is by the design and qualification of equipment; reducing the susceptibility of sensitive electronic components to the EMI/RFI hazard. As a consequence the SSCs are protected from design basis EMI/RFI hazards and there is no bounding fault in the Topic Report on Fault Assessment [Ref-17].

The Topic Report of Electro Magnetic Interference [Ref-8] presents an assessment of the EMI/RFI internal hazards for the UK ABWR and an introduction to the engineering topics to ensure electromagnetic compatibility (EMC).

7.10.2 Claims and Arguments

For most Internal Hazards, provision of the Fundamental Safety Functions is achieved through redundant and diverse trains of safety systems which are sufficiently segregated such that an Internal Hazard cannot prevent the delivery of the Fundamental Safety Functions. The approach to ensuring that and EMI/RFI hazard does not prevent delivery of the Fundamental Safety Functions is different in that the physical divisional barriers providing segregation of the divisions and the physical separation that provide protection from other Internal Hazards may not be so effective against the EMI/RFI hazard, with interactions between equipment possible through the walls of buildings or carried by cables which pass between different areas of the plant.

This leads to the following safety claim and arguments specific to EMI/RFI hazards. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH_E_SFC_5-7.1: General EMI/RFI claim
Any design basis EMI/RFI event originating from the UK ABWR GDA site will not prevent delivery of any required Fundamental Safety Functions.

(IH_E _SFC_5-7.1.A1)
EMC design principles are used to ensure that electrical and C&I equipment including associated cables are designed and installed so as to withstand the electromagnetic environment in the nuclear power plant. Section 7.10.3.2 presents further details on the EMC design principles used in the UK ABWR. These EMC Design Principles are presented below:

- Sources of EMI/RFI present in the UK ABWR can be identified and characterised using a systematic methodology based on standards and good engineering practice. The effects and risk of EMI/ RFI are identified through the application of international standards that provide information on the classification of electromagnetic environments and the determination of acceptable system response/recovery criteria.

  Section 7.10.3.3 presents further details on the sources of EMI/RFI Hazards in the UK ABWR and their potential consequences.

- To ensure EMC, a hierarchy of measures is identified, selected and implemented based, as a minimum, on relevant international standards.

  Section 7.10.3.4 presents further details a hierarchy of measures to ensure EMC.

- Through the application of the EMC design principles, international standards and relevant good practice risk is adequately mitigated.

(IH_E _SFC_5-7.1.A2)
Assessment of a postulated Design Basis EMI/ RFI Hazard has been performed, and based on this there is confidence that the GDA design is ALARP.

Section 7.10.4 presents a summary of the GDA assessment a postulated design basis EMI/RFI hazard, whilst Section 7.10.5 presents the ALARP discussion for EMI/RFI hazards.

7.10.3 Design Basis

7.10.3.1 EMI/RFI Hazard Analysis Methodology

The methodology developed in [Ref-8] for assessment of the EMI/RFI hazard includes the following steps:

(1) Definition of the area considered.
(2) Identification of potential sources of EMI/RFI.
(3) Identification of SSCs required for safety.
(4) Assessment of EMI/RFI consequences.
(5) As Low As Reasonably Practicable (ALARP) assessment.

Note that the consideration of consequences of a hazard is not limited to the room of origin, due to the nature of EMI/RFI which is likely to pass between rooms.

7.10.3.2 Design requirement

Hitachi-GE have developed the EMC design principles that should be considered in the design and installation of Electrical and C&I equipment in the UK ABWR:

- Sources of EMI/RFI present in the UK ABWR can be identified and characterized.
- Effects and risk of EMI/RFI are identified.
- A hierarchy of measures is identified, selected and implemented.
- Justification that risk is adequately mitigated.

7.10.3.3 Sources of EMI/RFI Hazards and Effects of EMI/RFI

Systematic identification of internal EMI/RFI sources that can be expected in the UK ABWR is shown as follows. Potential sources of internal EMI/RFI are categorised as natural and man-made sources based on the definitions in the IEC TR 61000-1-1 [Ref-43].

- Natural sources
  - Lightning/solar flare surge (note that this is categorised as an external EMI source),
  - Electrostatic discharge (ESD), etc.

- Man-made sources
  - Intentional sources
    - ✓ Portable communication devices
      - Mobile phones, Radio transceivers,
      - Portable electronic devices and computers, etc.
    - ✓ Wireless Local Area Network (WLAN)
  - Unintentional sources
    - ✓ Electrical equipment
      - Electric motor , Generator, Transformer,
      - Power cable,
      - Arc welding, etc.
    - ✓ Power system switching transients (under both normal and fault conditions)
      - Circuit breaker,
      - Inverter,
      - Thyristor,
      - Relay, etc.

The characteristics of each EMI/RFI source are determined. Characteristics include, but are not limited to, the following:

- Installation location.
- System.
- Power and frequencies (Inverter equipment).
- Radiated/conducted sources (which could include sources outside of the building/room being considered).

In the deterministic case, it can be assumed that the EMI/RFI source can affect electrical systems within the building/area that have particular susceptibility.

7.10.3.4 Electromagnetic Compatibility (EMC)

Generally, the basic principle to achieve EMC is to consider both the suppression of emission noise from sources (in other words, reducing EMI/RFI) and reduce the susceptibility to exogenous noise of potential receptors (in other words, reducing Electromagnetic Susceptibility (EMS)).

The basic principle to achieve EMC can be further developed to the following hierarchy of measures:

- Suppression of emission noise and mitigations
- Suppression of noise on transmission route
- Immunity to exogenous noise

Suppression of emission noise is achieved through the use of appropriate separation distances between the noise sources and sensitive electronic equipment; appropriate earthing and shielding of the noise sources.

Suppression of noise transmitted via the electrical connections (transmission route) is achieved through the separation of cables by raceways (cable ladders, conduits, etc.) according to voltage levels and signal levels of the circuits; using enclosed raceways for instrumentation cables; using shielded cables or twisted pair cables which are less susceptible to noise and the earthing of raceways.

To reduce the susceptibility to exogeneous noise, countermeasures at the end of the cable connecting to the equipment, and at the input port of the equipment can be used (e.g. shielding and earthing etc.). In addition, filters may be implemented to prevent the propagation of electromagnetic noise where required.

7.10.3.5 Combined Hazards

With the exception of lightning induced events other internal and external hazards do not induce EMI/RFI effects. EMI/RFI has the potential to cause faults in susceptible electronic equipment, but does not induce other internal (or external) hazards. Hazard combinations with EMI/RFI therefore do not need to be considered further.

7.10.4 Safety Evaluation

Potential sources of EMI/RFI and Electrical SSCs important to safety for each building have been identified in [Ref-8]. Qualification requirements will be determined during the detailed design phase based on analysis of the information on conditions for placing. The equipment will then be subject to an appropriate design and qualification programme.

7.10.4.1 EMI/RFI Consequence Assessment in GDA

[Ref-8] includes an assessment of a representative EMI/RFI case for the purposes of GDA assessment. The representative case was determined based on a number of parameters including intensity, safety function and distance using the design document of GDA, relevant good practice and engineering judgment. The assessment has followed the steps presented above and demonstrates that the approach to achieving EMC can be successfully applied during the detailed design phase.

7.10.4.2 EMI/RFI Consequence Assessment in Detailed Design

During detailed design, when the details of equipment locations and cable routing are defined, it will be necessary to perform a refined assessment. The objective of which will be firstly to ensure that the risk of EMI/RFI for each relevant SSCs is assessed, and then that adequate measures and mitigations are put in place to ensure the risk is reduced to ALARP.

In most cases it is anticipated that the justification that best practice in design has been applied, particularly with the adherence to IEC standards, will be sufficient, therefore the risk is managed by design, installation, commissioning, operation and any appropriate maintenance activity.

In cases where an EMI/RFI risk may be considered to be exceptional; such as proximity to very high currents, high voltage fields etc., a more detailed justification may be required with additional counter measures introduced as necessary.

7.10.5 ALARP Discussion

Equipment required to deliver Fundamental Safety Functions are physically separated to reduce the potential for common cause failure resulting from an EMI/RFI hazard. In accordance with relevant good practice, equipment will be designed to appropriate EMC standards (e.g. the IEC 61000 series) and qualified to an appropriate level to ensure EMC.

Assessment of a postulated bounding design basis EMI/RFI event has shown that the approach to assessing EMI/RFI Hazards and ensuring acceptable system response/recovery described above can be achieved during the detailed design phase.

A number of defence in depth measures have been identified to ensure that the UK ABWR design is ALARP with regards to the EMI/RFI hazard. Identification of design, operational and maintenance policies will be implemented to ensure EMI/RFI is minimised and the risk is mitigated.

It is concluded that the UK ABWR design meets relevant good practice to either prevent EMI/RFI sources or qualify equipment against their consequences such that risks are ALARP.

7.10.6 Conclusions

The UK ABWR is designed to prevent the EMI/RFI hazard from affecting any safety categorised equipment. Protection against this hazard is achieved by segregation and separation of systems, supported by an appropriate design and qualification programme.

It is considered that the EMI/RFI hazard will not prevent delivery of the Fundamental Safety Functions and will enable the safe operation of the UK ABWR by applying the content mentioned above and appropriate EMI/RFI standards.

7.11 Miscellaneous Internal Hazards

7.11.1 Introduction

The Topic Report on Miscellaneous Internal Hazards [Ref-9] addresses hazards which are not considered to be a major risk to the station but nevertheless need to be considered in the safety case. Following a scoping exercise discussed in Section 7.2.2, the following miscellaneous hazards are considered relevant for the UK ABWR:

- On-site Hazardous Materials.
- Transportation Accidents.
- Pipeline Accidents.
- Natural gases from the ground, e.g. Methane Hazards.

On-site pipeline accidents fall into the following categories and have already been assessed in the specific hazard analyses summarised above:

- Pipe Whip / Jet Impact (Section 7.6).
- Fire/Explosion (Section 7.4).
- Flooding (Section 7.5).

As a consequence, pipeline accidents are not discussed further in this Section.

There are some gases which are not contributors or products of the UK ABWR GDA process, but may be present within the site boundary originating from the ground. The potential for methane hazard has been identified in the GDA design, since it may occur due to organic material in the ground, e.g. peat and this topic must be considered in the detailed design phase. Should the methane hazard be identified on the proposed site, it will be necessary to identify measures to protect plant from the risk of explosion or asphyxiation due to accumulation of methane. Another naturally occurring gas is radon, and as discussed for methane, the detailed design will need to include measures to manage this. However, the GDA design does not preclude any options that the future licensee may select if these natural gases were present on the proposed site.

A comprehensive Hazard Schedule, containing all miscellaneous hazard events identified, is presented within the Topic Report on Miscellaneous Internal Hazards [Ref-9]. All hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.11.2 On-site Hazardous Materials

On nuclear facilities, there are a number of gases, acids, alkalis and solvents whose release could affect the delivery of the Fundamental Safety Functions. In the case of a number of these chemicals, a large release could affect operators in the safety classified buildings and prevent them from carrying out tasks related to nuclear safety. This includes considering any potential for asphyxiation

due to faults with the AC/ HVAC system which maintains the nitrogen atmosphere in PCV. Hence the location of hazardous chemical storage areas in relation to buildings containing safety classified SSCs and in particular the MCR are carefully chosen. The hazard analysis considers the consequences of major releases and the subsequent effects of gas releases on personnel and on plant equipment functionality.

7.11.2.1 Hazardous Materials Claims and Arguments

As for all other Internal Hazards, a principal objective of the hazardous material safety case is to limit the effects of any release of hazardous material to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5 and supported by the following claims and arguments specific to hazardous materials. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH_HM_SFC_5-7.1: Any Hazardous Material permitted on-site within the design basis will not prevent delivery of the Fundamental Safety Functions.

Claim IH_HM_SFC_5-7.1.1: Limiting the Sources of Hazardous Materials.

(IH_HM_SFC_5-7.1.1.A1)
Hazardous materials will be limited as far as reasonably practicable during the detailed design phase of the ABWR design. The GDA design does not assess all areas of the ABWR design and therefore cannot reduce the hazardous materials in areas not yet assessed. Section 7.11.2.2.3 discusses the sources of hazardous materials identified at GDA.

Claim IH_HM_SFC_5-7.1.2: Where possible locating the hazardous materials outside the safety classified area.

(IH_HM_SFC_5-7.1.2.A1)
There are no asphyxiate gases present within the MCR and the HVAC system is considered that hazardous materials located outside of the MCR cannot prevent FSFs being delivered by either SSCs or operators. Section 7.11.2.2.6 describes how the MCR HVAC mitigates the consequences of a gaseous hazardous material release.

Claim IH_HM_SFC_5-7.1.3: Designing systems which use or store hazardous materials to appropriate standards.

(IH_HM_SFC_5-7.1.3.A1)
Hazardous material release is prevented by use of appropriate design codes and operating procedures as discussed in Section 7.11.2.2.4.

Claim IH_HM_SFC_5-7.1.4: Mitigating the consequences of hazardous materials release.

(IH_HM_SFC_5-7.1.4.A1 & IH_HM_SFC_5-7.1.4.A2)
Liquid hazardous materials do not prevent delivery of the FSF as sufficient EMIT regimes will be defined at the detailed design phase such that SSCs will not be damaged to the extent where FSFs would not be able to be delivered. Any consequences due to immersion are bounded by the immersion flooding assessments presented within the Topic Report on Internal Flooding [Ref-3].

These arguments are discussed further in Section 7.11.3.3.

7.11.2.2 Hazardous Materials Design Basis

7.11.2.2.1 Hazard Analysis Methodology

The methodology developed for assessment of Hazardous Materials includes the following steps:

(1) Hazardous materials, their quantities, physical form and storage locations on -site have been identified (see the Topic Report on Miscellaneous Hazards [Ref-9] for details).
(2) Small volumes of hazardous materials used during normal operations and materials identified for use during decommissioning are screened out at this time. Decommissioning is discussed in more details in PCSR Chapter 31.
(3) For the remaining materials (large volumes of stored liquids and gases), credible releases are assessed and their potential consequences determined.
    (a) In the case of stored liquids two separate effects may occur, as follows:
        (i) flooding hazard – this would have a prompt effect, however a comparison against the bounding flood hazard in the same area/ room has shown that the flooding by hazardous liquids is bounded (as flooding within a division is assumed to lead to the loss of function of the A-1 SSCs within that division, this bounds any consequences that may occur from the hazardous material).
        (ii) Corrosion hazard – this is screened out since the corrosion effects are gradual and action is taken to drain the corrosive before significant damage is sustained.
    (b) In the case of stored gases, none of the gases used in the ABWR are corrosive and there will be no challenge to SSC performance. Carbon Dioxide and Nitrogen are, however, potential asphyxiants and their impact on the following systems is considered:
        (i) HVAC for MCR in C/B
        (ii) EDGs in EDG/Bs and
        (iii) BBGs in B/B.

    To prevent oxygen displacement due to nitrogen release or other gas release, the HVAC air intakes for the various identified systems take air directly from the atmosphere outside of the buildings, from an elevated location. It is not considered credible that leakage from either location could cause a sufficiently depleted oxygen level at any important SSC locations to prevent delivery of safety functions.

7.11.2.2.2 Design Requirement

The hazardous material claims in Section 0 will be achieved in the UK ABWR by:

- Limiting the sources of hazardous materials.

- Where possible locating the hazardous materials outside the safety classified buildings.
- Designing systems which use or store hazardous materials to appropriate standards.
- Mitigating the consequences of hazardous materials release.

7.11.2.2.3 Sources of Hazardous Materials

As discussed in [Ref-9], in general any significant quantities of materials are located in dedicated bottle stores and not within the safety classified buildings. The exception to this are hazardous materials in low quantities and nitrogen supplies to various systems in the R/B. Hazardous materials of a low quantity within safety classified buildings do not prevent the delivery of the Fundamental Safety Functions. The on-site hazardous materials can be grouped into the following three categories:

- Hazardous materials not within safety classified buildings.
- Nitrogen within the R/B.
- Transient and permanent hazardous materials of a low quantity within safety classified buildings.

7.11.2.2.4 Prevent Hazardous Materials Release

The storage and use of certain chemicals will comply with relevant UK/ EU regulations such as the Registration, Evaluation, Authorisation and restriction of Chemicals (REACH) regulations (EC 1907/2006) and the Chemical Labelling and Packaging regulations (CLP) when enacted in UK.

In addition, depending on site specific requirements, compliance with the Control of Major Accident Hazards (COMAH) Regulations, 2015 may be required if the quantities of hazardous materials stored exceed the specified thresholds within the regulations. These regulations require the operator to take the necessary measures to prevent major accidents involving dangerous substances and to limit their consequences to persons and the environment, including preparation of emergency plans. Control of chemicals on site will also comply with the Control of Substances Hazardous to Health (COSHH) Regulations 2002.

Hazardous materials delivered to site become an Internal Hazard as soon as they are within the site boundary, and the hazards associated with their transport on-site are considered. However it is noted that the transport of these materials will comply with the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009.

7.11.2.2.5 Combined Hazards

No combined hazards combinations have been identified.

7.11.2.2.6 Mitigate Consequences of a Hazardous Materials Release

Following a hazardous material release the operators within the MCR may be required to assist in the delivery of the Fundamental Safety Functions [Ref-17].

The MCR HVAC systems are independent from HVAC systems outside the MCR compartment, during normal operation and normal shutdown all MCR HVAC equipment is in operation. This allows the SSCs and operators within the MCR to provide any required FSFs within the design environmental conditions. There are no asphyxiate gases present within the MCR compartment and the MCR HVAC intakes are located on the roof of the C/B ensuring that hazardous materials released outside of the MCR compartment cannot prevent delivery of the FSFs by either SSCs or operators within the MCR.

7.11.2.3 Safety Evaluation

Hazardous materials within the R/B and C/B are of such a low quantity that it is judged that they will not affect the SSCs or prevent personnel from carrying out operations which assist in the delivery of Fundamental Safety Functions. Potentially corrosive materials are used in small quantities and any spillage would be expected to be cleaned up before any adverse consequences occur.

Larger volumes of hazardous materials are present in the T/B and EDG/Bs (lubricating and fuel oils), however the quantities are significantly smaller than the credible flooding sources in these buildings and the consequences of immersion in oil are bounded by the immersion flooding assessments in Section 7.5. As shown in Section 7.5, there are no consequences that challenge the delivery of the Fundamental Safety Functions.

There are no safety classified SSCs which can be affected by a hazardous material release within and outside safety classified buildings. Therefore there are no consequences which challenge the delivery of the Fundamental Safety Functions.

7.11.2.4 Hazardous Material ALARP Discussion

Inventories of hazardous materials have been reduced as far as reasonably practicable. The tanks, vessels and/ or pipework in which the hazardous materials are stored have been designed in accordance with the relevant good practice and, as a minimum, UK Standards.

As applicable, tanks/ vessels holding hazardous materials, which are subject to COMAH regulations, will undergo regular inspection/ testing to confirm the continued integrity and suitability.

Storage locations and engineered features (e.g. the MCR HVAC air inlet structure) are such that the consequences of a hazardous material release are mitigated as far as is reasonably practicable.

It is concluded that the UK ABWR design meets relevant good practice in respect to the management of hazardous materials and that the risks from a hazardous material release are ALARP.

7.11.3 Transportation Accidents

At nuclear installations material and equipment are moved using a variety of forms of transport. If transport movements are not adequately controlled there is a potential for collision/impacts that could have implications for nuclear safety.

7.11.3.1 Transport Accidents Claims and Arguments

As for all other Internal Hazards, a principal objective of the transport accident safety case is to limit the effects of any transport accident to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5 and supported by the following safety claims and arguments specific to transport accidents. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH_TA_SFC_5-7.1: Transport Accident events within the design basis will not prevent delivery of the Fundamental Safety Functions.

Claim IH_TA_SFC_5-7.1.1: A design basis transport accident occurring outside of a safety classified building will not prevent the delivery of the Fundamental Safety Functions.

(IH_TA_SFC_5-7.1.1.A1)
SSCs supporting the delivery of the FSFs are sufficiently segregated/located within safety classified buildings or with sufficient protective measures as such to be protected from the consequences of transport accidents originating within the Yard.

Claim IH_TA_SFC_5-7.1.2: A design basis transport accident occurring within a safety classified building will not prevent the delivery of the Fundamental Safety Functions.

(IH_TA_SFC_5-7.1.2.A1)
Vehicle access to safety classified buildings are limited to the R/B, T/B, Rw/B and Hx/B and limited to specific areas within buildings.

7.11.3.2 Design Basis

7.11.3.2.1 Hazard Analysis Methodology

The methodology developed for assessment of Transport Accidents includes the following steps:

1. Identification of potential sources of a transport accident, for GDA this is the representative vehicles discussed above.
2. Assessment of transport accident event.

7.11.3.2.2 Design Requirement

The transport accident claims in Section 0 will be achieved in the UK ABWR by:

- Controlling site access to vehicles required to support operations.
- Controlling the speed and travel paths of vehicles on site.
- The robust construction of the safety classified buildings.
- The provision of local crash barriers where required to protect SSCs from impact.

7.11.3.2.3 Sources of Transport Hazards

There are numerous transports carried out on the ABWR site, particularly during outage periods. For the purposes of this assessment accidents are divided into two classes, those that occur outside of safety classified buildings and those that occur within safety classified buildings.

A full list of vehicle movements will be developed to support the site specific PCSR. This will assist in developing a comprehensive transport accident assessment by assessing the worst case vehicle impact events (e.g. largest vehicle, heaviest vehicle, loads being carried, routes, frequencies of movement, etc.). For GDA, a representative selection of vehicle types has been determined. These are medium (10 ton) and large (20 ton) lorries that will access to loading bays within buildings; cranes (30 to 45 ton) and emergency services vehicles (up to 30 ton) that will operate adjacent to the outer walls of buildings.

7.11.3.2.4 Prevent Transport Accidents

Transport accidents are prevented by provision of safe routes for all material movements on site, suitable operating restrictions (e.g. speed restriction and access restriction via security controls) and the use of suitably trained and experienced operators.

7.11.3.2.5 Combined Hazards

The Combined Internal Hazards assessment [Ref-14], has determined that due to the robustness of the building structures and the features present in vehicle access areas of the safety classified buildings that these consequential hazards will be very unlikely and the combined hazard does not require further assessment.

7.11.3.3 Safety Evaluation

There are no A-1 safety classified SSCs which have Fundamental Safety Functions outside of the safety classified buildings. Therefore, only transport accidents associated with the following safety classified buildings are considered in this assessment for GDA Step 4 are:

- Reactor Building (R/B).
- Turbine Building (T/B).
- Heat Exchanger Building (Hx/B).
- Radwaste Building (Rw/B).

It is noted that the C/B is not considered in this assessment as it is protected on all sides by other building structures and there is no vehicular access route. The B/B, S/T, EDG/B and S/B do not have vehicle access and are not considered in this assessment Access to the FV/B is via the R/B and therefore included in the R/B assessment.

Transport accident external to the safety classified buildings
Detailed assessment of vehicle impacts upon buildings is beyond the scope of GDA, as this requires information on site layout and access roads. However, it is judged that any credible accidental external vehicular impacts to civil structures will not result in dynamic loads capable of affecting any SSCs performing FSFs within the buildings. This will be demonstrated during detailed design phase when detailed layout information is available. Where it cannot be demonstrated that civil structures will protect SSCs performing FSFs within the buildings from the dynamic loads of the vehicle impact, further mitigation will be considered. This could include consideration of new road layouts, transit routes, barriers to protect vulnerable buildings, etc.

Although a detailed assessment cannot be completed during the GDA phase of work there are a number of measures that can be considered, these are:

- The speed and travel paths of vehicles will be controlled and monitored using appropriate procedures commensurate with the consequences of an operator error.
- Consideration will be given to having more onerous operating restrictions if there is potential for multiple vehicles to be moving in the same area at the same time.
- When appropriate vehicles will be provided with automatic systems to prevent operation outside the design basis envelope.
- When a possibility exists that an impact might reasonably occur having a nuclear consequence, appropriately designed energy absorbing barriers will be provided. The design specification will also allow for vehicles operating outside of their normal procedures.

In addition a general site speed restriction will be imposed to limit vehicle speeds and where appropriate specific transports will have a lower speed restriction. It is noted that there may be scenarios where safety measures are introduced to mitigate other hazards that offers some or complete protection from transport-type hazards, e.g. the collision of vehicles into the reactor building may be bounded by aircraft impact. Other buildings will be assessed on a case-by-case basis, however it should be noted that all safety classified buildings are seismically qualified and so will be robustly constructed.

Transport accidents largely occur due to human error. Therefore it is not possible to remove the internal hazard of transport accidents from the UK ABWR design. The use of SQEP operators, banksmen, operational procedures and training limits the effect of human error on transport accidents.

Transport accident internal to the safety classified building
Vehicle access to safety classified buildings is limited to the R/B, T/B, Rw/B and Hx/B. Vehicle access to the T/B, Rw/B and Hx/B is only during outage and only the large component entrance within the R/B is accessed during power operation. During outages only a single safety division is out for maintenance and vehicle access is only to that division in maintenance where a building is segregated divisionally.

Access to the R/B is via the large component entrance which is fitted with a pair of interlocked double doors at either end, which are termed the internal and external doors. When not in use, the

external doors remain closed and make up part of the secondary containment of the R/B. When the exterior doors are open the interior are shut and form the secondary boundary. Operational procedures require that only the internal or external doors are open at any one time. A road vehicle entering or exiting the large component entrance will therefore have to stop for health physics checks prior to the secondary doors being opened. The vehicle speed when entering this area will be minimised and the maximum speed that a vehicle could achieve prior to impacting an internal structure would therefore be low.

Access to the T/B is limited to specific areas of the building. Vehicles cannot enter areas where A-1 SSCs are located. Therefore a vehicle impacting a SSC which is required to deliver any FSFs is not a credible event. It is noted that there are no FSFs delivered within the T/B during outage operations as the main steam turbine and any supporting systems are isolated i.e. the Off Gas system.

The Rw/B does not contain any safety classified SSCs therefore the delivery of the FSFs can be achieved following a vehicle accident within the Rw/B. It is noted that detailed design of the Rw/B is under development and therefore vehicular interactions with the Rw/B will be reassessed during the detailed design phase.

The Hx/B is fully segregated during outage and therefore only one division will be accessed for maintenance at any one time. Vehicular access to the Hx/B is limited and vehicles are segregated from A-1 SSCs that may be required to deliver FSFs following a vehicle accident.

It is noted that the assessment of transport accidents is limited within GDA, due to the detail available regarding vehicles and access routes. Further detailed assessment will be conducted during the subsequent design phase.

7.11.3.4 Transport Accident ALARP Discussion Transport Accident ALARP Discussion

Transport accidents largely occur due to human error. Therefore it is not possible to remove the internal hazard of transport accidents from the UK ABWR design. Vehicle movements on site are subject to speed restrictions which will greatly reduce the likelihood and consequences of accidents occurring. In addition, the use of SQEP operators, banksmen, operational procedures and training limits the effect of human error on transport accidents.

Vehicle impact barriers can be provided at locations where either safety essential buildings could be impacted or where vehicles are more likely to have an accident (e.g. bends or narrow passages). This is dependent on site layout, and is thus beyond the scope of GDA. The requirement for any barriers to provide additional protection to buildings will be determined during the detailed design phase.

It is concluded that the UK ABWR design meets relevant good practice in respect to the management of transport vehicles and that the risks from a transport accident are ALARP.

7.11.4 Conclusions

There are no safety classified SSCs which can be affected by a hazardous material release within and outside safety classified buildings. In addition, robust structures of the safety classified buildings, controls on vehicle movements and the equipment layout ensure that transport accidents cannot impact safety classified SSCs.

There are no consequences from either hazardous materials or transport accidents which challenge the delivery of the Fundamental Safety Functions.

7.12 Primary Containment Vessel (PCV)

7.12.1 Introduction

The Topic Report on Internal Hazards in the Primary Containment Vessel [Ref-10] considers the internal hazards that could affect exception to segregation SSCs located within the PCV.

The PCV is comprised of a cylindrical RCCV situated in the centre of the R/B which is capped by the drywell (D/W) head. The drywell head cap is removed to provide access to the RPV during refuelling outage. The PCV forms the primary containment boundary and encloses the RPV, D/W, Suppression Chamber (S/C) and S/P.

The PCV contains components of systems which ensure safe operation of the reactor. These include the reactivity control systems such as the CRD and components of the Standby Liquid Control system (SLC); components of the Reactor Coolant System (RCS); engineered safety systems in order to suppress or prevent fuel damage or the potential discharge of large amounts of radioactive substances in the event of faults, incidents or accidents, including the Emergency Core Cooling Systems (ECCS); and instrumentation to monitor the key parameters in the RPV and PCV.

See PCSR Chapters 12: Reactor Coolant Systems, Reactivity Control Systems and Associated Systems, and 13: Engineered Safety Features, for more details on these systems.

As discussed in Section 7.3.1.9 there is no divisional segregation within the PCV and therefore a different assessment methodology has been applied to demonstrate that Internal Hazards within the design basis will not prevent the delivery of the Fundamental Safety Functions [Ref-10].

For the PCV, the following hazards are included in the design basis assessment [Ref-15]:

- Fire and Explosion.
- Internal Flooding.
    - Immersion.
    - Spray.
    - Steam Release.
- Pipe Whip and Jet.
- Dropped and Collapsed Loads.
- Internal Missiles.
- Blast.
- EMI (this is addressed through all buildings assessment as discussed in Section 7.10).

A comprehensive Hazard Schedule, containing all bounding hazard events identified, is presented within the Topic Report on Internal Hazards in the Primary Containment Vessel [Ref-10]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

It should be noted that hazards associated with the RPV are not assessed within the Internal Hazards topic area.

7.12.2 Claims and Arguments

The PCV contains SSCs from all four C&I divisions and as such is an area of exception to segregation. General Claim IH_SFC_5-7.3 is considered to apply to the PCV.

General Claim IH_SFC_5-7.3: Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after an Internal Hazard, to fulfil the Fundamental Safety Functions.

This general claim is supported by lower level more detailed (hazard specific) claims and arguments below which together demonstrate the higher level claim has been achieved.

Claim IH_FE_PCV_SFC_5-7.3: Any Design Basis **Internal Fire or Explosion event originating within the PCV will not prevent delivery of the Fundamental Safety Functions**

(IH_FE_PCV_SFC_5-7.3.A1)
Quantities of flammable materials in the PCV are minimised and controlled. During normal power operations, there will be an inert gas blanket within the PCV that provides a defence-in-depth means to prevent fires. In addition, the PCV structure is capable of withstanding the design basis fire.

(IH_FE_PCV_SFC_5-7.3.A2)
Radiolytic hydrogen in pipes and components within the PCV will be below 25% LFL which eliminates the risk of hydrogen explosion during normal power operations.

(IH_FE_PCV_SFC_5-7.3.A3)
The potential pool fire would not affect SSCs performing category A functions due to the significant spatial separation.

(IH_FE_PCV_SFC_5-7.3.A4)
The electrical and physical separation of cables prevents spreading of fire to other divisions or from the inside to the outside of the PCV.

These arguments are discussed further in Section 7.12.4.1 (Fire and Explosion inside the PCV)

Claim IH_ F_PCV_SFC_5-7.3: Any Design Basis Internal Flood event originating within the PCV will not prevent delivery of the Fundamental Safety Functions

(IH_F_PCV_SFC_5-7.3.A1)
Flooding hazards in the PCV, including spray and steam release, are bounded by a large break leading to a LOCA inside the PCV.

(IH_F_PCV_SFC_5-7.3.A2)
The PCV structure is capable of withstanding a design basis LOCA.

(IH_F_PCV_SFC_5-7.3.A3)
All equipment and cabling required to be operable or maintain a safe state during and after a LOCA are designed and qualified to withstand the harsh conditions inside the PCV.

(IH_F_PCV_SFC_5-7.3.A4)
During outages, when the hatches to equipment tunnels will be open, a LOCA below the TAF will not propagate to the R/B as the hatches can be closed before the water overflows from the PCV to R/B.

These arguments are discussed further in Section 7.12.4.2 (Flooding Inside the PCV)

Claim IH_ PJ_PCV_SFC_ 5-7.3: Any Design Basis Internal Pipe Whip or Jet event originating within the PCV will not prevent delivery of the Fundamental Safety Functions

(IH_PJ_PCV_SFC_5-7.3.A1)
The PCV liner and RC structure is capable of withstanding a design basis Pipe Whip and Jet Impact event.

(IH_PJ_PCV_SFC_5-7.3.A2)
Spatial separation of safety divisions within the PCV and other mitigations are available as a means to prevent multiple pipe impacts and redundancy of isolation valves outside PCV ensures that a suitable combination of Class 1 SSCs or a secondary line of protection always remains operable and capable of delivering the FSFs following a pipe whip fault.

These arguments are discussed further in Section 7.12.4.3 (Pipe Whip and Jet Impact inside the PCV)

Claim IH_ D_PCV_SFC_ 5-7.3: Any Design Basis Dropped Load event originating within the PCV will not prevent delivery of the Fundamental Safety Functions

(IH_D_PCV_SFC_5-7.3.A1)
Spatial separation of safety divisions within the PCV ensures a suitable combination of Class 1 SSCs always remains operable and capable of delivering the FSFs following a dropped load event. Heavy lifts within the PCV will only be undertaken during outages.

This argument is discussed further in Section 7.12.4.4 (Dropped Loads inside the PCV)

Claim IH_CM_PCV_SFC_5-7.3: Any Design Basis Internal Missile event originating within the PCV will not prevent delivery of the Fundamental Safety Functions

(IH_CM_PCV_SFC_5-7.3.A1)
Design Basis Missile hazards are confined within the PCV and the upper D/W hatch room. The DWC fan casing will withstand the postulated impeller missile.

(IH_CM_PCV_SFC_5-7.3.A2)
There may be multiple deflections of a condensing chamber missile from the RPV or reactor shield wall. However the annular distribution and vertical separation of condensing chambers makes it

unlikely that damage would occur to sufficient chambers to prevent delivery of the RVI system safety function.

(IH_CM_PCV_SFC_5-7.3.A3)
Spatial separation of safety divisions within the PCV and redundancy of isolation valves outside PCV ensures that a suitable combination of Class 1 SSCs or a secondary line of protection always remains operable and capable of delivering the FSFs following any design basis missile.

These arguments are discussed further in Section 7.12.4.5 (Missiles inside the PCV)

Claim IH_B_PCV _SFC _5-7.3: Any Design Basis Blast event originating within the PCV will not prevent delivery of the Fundamental Safety Functions

(IH_B_PCV_SFC_5-7.3.A1)
Spatial separation of safety divisions within the PCV ensures a suitable combination of Class 1 SSCs always remains operable and capable of delivering the FSFs following a blast event. The reactor shield wall will confine the pressure wave from a blast associated with the condensing chambers.

This is discussed further in Section 7.12.4.6 (Blast inside the PCV)

Each identified internal hazard has been assessed to demonstrate that there is sufficient spatial and electrical separation of redundant SSCs within the PCV capable of delivering the FSFs.

7.12.3 Design Basis

The Internal Hazard assessment methodology inside the PCV follows the same general approach as that for Internal Hazards outside the PCV:

(1) Identify safety classified SSCs to be protected.
(2) Identify sources of Internal Hazards inside PCV.
(3) Characterise the Internal Hazard, including evaluating the damage potential to SSCs.
(4) Identification of available SSCs to ensure delivery of the FSFs following an internal hazard.

Although much of the same approach for outside of PCV does apply, the emphasis at each stage of the assessment differs. Within the PCV segregation is not possible due to the different Class 1 divisions converging, therefore, General Claim IH_SFC_5-7.2 cannot be applied. Protection against Internal Hazards is based upon separation and/or qualification of SSCs against any relevant Internal Hazards to support safety claim IH_SFC_5-7.3. This is summarised as follows:

- Hazard prevention.
- Spatial separation of redundant SSCs.
- Qualification of equipment.
- Engineered Measures.
- Administrative Measures.

The assessment methodologies for each Internal Hazard are similar to the equivalent methodologies outside of the PCV presented above. However, the methodologies necessarily differ in the assessment of damage potential as the pessimistic assumption of loss of all SSCs within a hazard compartment used in the individual hazard analyses above is not appropriate when evaluating these exception to segregation SSCs.

7.12.4 Safety Evaluation

The PCV is identified as an area of exception to segregation as the hazard separation division contains multiple Class A-1 division SSCs in a large open space without dedicated physical barriers between divisions. Redundant trains and penetrations are separated to maintain the safe operation of the plant in the event of a hazard. In general, all SSCs related to divisions I and III are located in the East half of the PCV, whilst divisions II and C&I division IV are located in the West half.

During an outage, the Class 1 SSCs from divisions I and II are under maintenance during the first half of outage. Class 1 SSCs from divisions III and IV are under maintenance during the second half of outage.

7.12.4.1 Fire and Explosion inside the PCV

The PCV is normally inerted with Nitrogen, however, the fire and explosion assessment has been performed assuming that inertion is not present. The assessment has identified lubricant oils as potential sources of a pool fire and cabling as potential sources of an electrical fire within the PCV. In both cases the combustible loads are very low and no credible fire scenarios have been identified that could affect the plant's delivery of FSFs.

[Ref-10] presents the analysis of potential pool fires and concludes that the fire would be localised and would not affect SSCs performing Category A functions due to the significant spatial separation present between fire source and these SSCs. Some cabling associated with the FMCRD or RIP motors (non-Class 1) and neutron monitoring is present in the area, and could conceivably undergo heating by a postulated pool fire in either fire scenario although flames are not expected to impinge on the cables.

[Ref-10] also presents the analysis of potential electrical fires. Safety class 1 cables in the PCV are installed in enclosed cable trays and metallic conduits [Ref-38], except for the small portions where the cables reach equipment, where open configurations might be used. Cables are run in dedicated divisional cable raceways and conduits, and are electrically and physically separated from other safety divisions. [Ref-10] concludes that the ignition of cabling does not pose a risk of fire propagating to other divisions or propagating from inside to outside of the PCV.

The potential for fire spreading outside of the PCV during an outage when hatches are open is also assessed in [Ref-10]. If temporary services need to be routed through hatches during an outage, groups of (fire retardant) cables will be separated by at least the minimum IEEE-384 distance to minimise the potential for fire spread. In addition risk assessments will be in place when introducing

any transient fire risks. There is no means for an internal fire in an electrical raceway to significantly spread from the source and propagate from an enclosed raceway to outside of the PCV through an open hatch.

The only explosion hazard in the PCV comes from radiolytic hydrogen accumulation in pipes, no other explosion hazard sources have been identified. The TR on the Safe Management of Radiolytic Gases Generated during Normal Operations [Ref-18] assesses the hazard inside the PCV and has demonstrated that there is no risk of hydrogen accumulation over 25% LFL in any of the pipes and components, and that there will therefore be no explosion from radiolytic hydrogen in normal operations in the PCV.

Based on the assessment above, it is concluded that a Design Basis Internal Fire or Explosion event originating within the PCV will not propagate beyond the PCV and will not prevent delivery of the FSFs.

7.12.4.2 Flooding Inside the PCV

As described in [Ref-10], flooding hazards in the PCV (including spray and steam release), are bounded by a large break leading to a loss of coolant accident (LOCA) in combination with operation of the RHR containment vessel cooling spray mode. In accordance with [Ref-39], all equipment and cabling required to be operable or maintain a safe state during and after a LOCA are designed and qualified to withstand the harsh conditions inside the PCV. At power operations the containment boundary will confine all flooding hazards within the PCV. All penetrations for piping, HVAC, electrical cabling and trays, as well as hatches for equipment and personnel access in the PCV form part of the primary containment boundary and (during power operations) are sealed with airtight and watertight requirements and designed to withstand the pressure, humidity and temperature conditions inside the PCV during and after LOCA conditions.

During outages the man access and equipment access hatches may be open. In general, any leakages from pipe failures or reactor well leak posing an immersion hazard would be collected in the S/P through the vent pipes. However, if a LOCA below the top of the fuel occurs during an outage the drywell will potentially flood. Based on the closure procedures for the man access and equipment access hatches, it will be possible to achieve closure of these hatches before any volume of flood water had entered the R/B.

7.12.4.3 Pipe Whip and Jet Impact inside the PCV

High energy pipe whip and jet impact within the PCV is most likely during power operations since during outages the water and steam systems in the PCV are depressurized, some small bore lines (<50mm) will be energised in outage, but these will not cause damage to important SSCs. Pipe whip and jet impact has the potential to result in impact on different SSCs, multiple components can be ruptured as a result of one event.

The pipe whip assessment in [Ref-10], has shown that the PCV liner and RC structure is capable of withstanding a design basis Pipe Whip and Jet Impact event and therefore the event would be contained within the PCV with no secondary hazards outside of the PCV.

The assessment shows that, due to the presence of the DEPSS, a single pipe whip movement is prevented from impacting on multiple pipes or significantly reduces the impact energy such that secondary pipe failures do not occur within the design basis. For the location where DEPSS is not available, it has been demonstrated that although direct pipe-to-pipe impact may occur, the impact energy is low enough that secondary failure is not credible.

The assessment also demonstrates that due to spatial separation of Class 1 divisions within the PCV, the use of robust pipe whip restraints and redundancy of isolation valves outside PCV, a suitable combination of A-1 and/or A-2 SSCs always remains operable and capable of delivering the Fundamental Safety Functions for pipe whip fault

7.12.4.4 Dropped Loads inside the PCV

Inside the PCV, lifting operations are only carried out during outage operations, thus no dropped loads assessment is carried out for power and low power operations inside the PCV.

The dropped load assessment in [Ref-10] shows that effect of a dropped load would be relatively localised. The drop of the heaviest component during lifting operations in the upper drywell has shown that the dropped load is unlikely to impact the reactor shield or containment liner. If an impact did occur, the damage to the shield would be superficial and there would be a negligible reduction in radiation shielding performance. Furthermore there is no functional requirement on the containment liner during outage.

Spatial separation between SSCs within the PCV ensures that, in case of a dropped load, systems from different divisions will not be affected and sufficient redundancy is provided to ensure that the FSFs continue to be delivered.

7.12.4.5 Missiles inside the PCV

Within the PCV there are potentially explosive systems, (e.g. vessels containing radiolytic hydrogen), pressurised systems (high energy pipes and vessels), and rotating machinery (fans and pumps) which can be sources of missiles in the event of their failure.

Analysis within [Ref-10] demonstrates that the only credible missile sources are the condensing chambers, the Safety Relief Valve (SRV) accumulators, Automatic Depressurisation System (ADS) accumulators and the Drywell Cooling System (DWC) fans.

There are 12 instrumentation condensing chambers located between the reactor shield wall and the RPV. Two types of condensing chamber are used with significant vertical spatial separation between the two types. In addition condensing chambers are distributed around the annulus such that only a small number of chambers are in direct line of sight from any missile source.

[Ref-10] demonstrates that the reactor shield wall and RPV are not penetrated by a condensing chamber missile and therefore missiles associated with a blast of a condensing chamber will be confined within the annulus between the reactor shield wall and the RPV. It is likely that there may be multiple deflections of a condensing chamber missile from the RPV or reactor shield wall, although the limited space between the RPV and the reactor shield wall will not allow the missile to impact a large area around the PCV, even after multiple deflections.

As a result of the significant vertical spatial separation between condensing chamber types, even if there were multiple missile deflections it would be unlikely to damage sufficient chambers to prevent delivery of the RVI system safety function. The probability of a deflection posing a threat to SSCs outside of the line of sight of the condensing chambers in one bounding plant impact zone will be low.

In the case of the SRV and ADS accumulators, [Ref-10] demonstrates that the missiles will not perforate the RCCV liner therefore the PCV containment function will not be compromised by any missile impact. An accumulator missile could result in secondary accumulator impacts and failures, however a suitable combination of A-1 and/or A-2 SSCs always remains operable and capable of delivering the FSFs following a design basis accumulator missile. During an outage when the upper D/W hatch is open, a missile could potentially escape the RCCV, however it could only reach the upper hatch room which contains no safety related equipment. There is no claim on the hatches during outage.

In the case of the DWC fans, the fan casing has been demonstrated in [Ref-10] to be sufficient to withstand the impact from the design basis missile. However, an analysis has been performed the potential consequences if no credit is taken for the fan casing. This analysis has demonstrated that, whilst missiles may lead to equipment damage, the spatial separation of SSCs within the PCV ensure that a suitable combination of A-1 and/or A-2 SSCs always remains operable and capable of delivering the FSFs following a DWC fan missile event.

7.12.4.6 Blast inside the PCV

Analysis within [Ref-10] shows that high energy pipes, the condensing chambers and SRV and ADS accumulators are credible blast sources within the PCV during power operations.

The PCV concrete containment is designed to withstand loads of dynamic nature and overpressures. As discussed above, the liner has been substantiated against pipe whip and missile impact. A pipe whip would represent a more onerous challenge to a barrier than a blast, and therefore it is concluded that the RCCV liner will accommodate blast pressures with no perforation.

Assessment of the overpressure as a function of distance from a high energy pipe blast has been performed in [Ref-10]. This has shown that the blast could only cause significant overpressure in one half of the PCV and that there is suitable separation of Class 1 SSCs within the PCV to ensure that least one division of the reactor safeguard systems would always be available.

Assessment of the overpressure as a function of distance from a condensing chamber blast has been performed in [Ref-10], this has shown that the blast could lead to localised equipment damage which may affect the functionality of the adjacent condensing chamber but would not lead to a consequential blast failure. Due to the distribution of the condensing chambers within the reactor shield wall, at least two Class 1 lines of protection remain unaffected following a design basis condensing chamber blast.

As with the consequences of missiles resulting from ADS or SRV accumulator failures, a design basis accumulator blast has the potential to result in secondary accumulator failures, however a suitable combination of A-1 and/or A-2 SSCs always remains operable and capable of delivering the FSFs following the design basis accumulator blast.

7.12.5 Consequential Hazards

No significant consequential hazards are identified due to the seismic and environmental qualification of SSCs, and significant spatial separation between A-1 SSCs.

7.12.6 ALARP Discussion

The design of the UK ABWR PCV has evolved from the existing J-ABWR design with a number of improvements to reduce risk from internal hazards, including equipment to facilitate supported lifts of heavy components for maintenance (see below). In addition, the robust component specifications are based on RGP, and examples are given below.
The flammable material inventory is very low and this is contained in the equipment and leakage would be collected in a sump. The cable design is based on fire retardant cables, adequate separation distances between raceways, and divisional electrical penetrations.

With respect to flood hazards, all equipment and cabling is designed and qualified to withstand the harsh environment in the PCV post LOCA initiation.

The high energy pipe work meets appropriate ASME standards represents worldwide best practice, and will ensure that the frequency of their failure is very low. This is supported by the DEPSS and robust pipe whip restraints for the key high energy pipes, which minimise the consequences of a postulated pipe whip event.

Dropped loads are only an issue during outages when heavy items such as MSIVs and SRVs will need to be removed for maintenance or replacement. Specialised handling equipment, a pneumatic jack and trolley system, for which the routing of the rails (run on the floor) are away from essential SSCs has been adopted as part of the UK ABWR.

As discussed above, the steel casing of the DWC fans are sufficient to contain a failed impeller. This will remove the potential for a large missile to be ejected and damage essential SSCs such as ADS accumulators and SRVs. Sufficient A-2 systems are available to support the A-1 ADS safety function. In the unlikely event of an ADS accumulator missile/ blast causing damage to adjacent

ADS accumulators, these provide the means to ensure depressurisation of the reactor and allow low pressure water cooling to be maintained.

It is concluded that the PCV layout and design generally meets relevant good practice to either prevent internal hazard sources or effectively mitigate their consequences such that risks are ALARP.

7.12.7 Conclusions

An Internal Hazard assessment has been performed for the PCV of the UK ABWR. Due to the lack of divisional barriers in the area, the hazards are assessed on a case by case basis. It is confirmed that due to the design of the redundant and diverse systems, there will always be sufficient A-1 and/ or A-2 SSCs available to deliver the Fundamental Safety Functions for all design basis hazards.

7.13 Main Control Room (MCR)

7.13.1 Introduction

The Topic Report on Internal Hazards in the Main Control Room [Ref-11] considers the internal hazards that could affect exception to segregation SSCs located within the MCR and its supporting rooms.

The primary purpose of the MCR and its supporting rooms (known collectively as CB-MCR) is to allow operators to monitor reactor plant in normal operation and in emergency scenarios. The UK ABWR design is based on automatic actuation of key safety systems for delivering FSFs, but CB-MCR provides the equipment for both the required monitoring of these systems and an alternative (manual) method of actuation. In addition a manual reactor scram function is provided, allowing operators to initiate manual emergency shutdown of the reactor.

To deliver these functions the MCR contains Human Machine Interfaces (HMI) for A-1 and A-2 SSCs, facilities for operators (the MCR is continuously occupied) and systems supporting the habitability of the plant in accident scenarios (independent HVAC etc.). The MCR also serves as a base for overseeing and supervising the release of plant for maintenance, directing field operator duties and providing initial control during site emergencies. It is expected that at any time the MCR will be crewed by two Control Room Operators (CRO) and a MCR Supervisor (MCRS) per shift. Further detail on crew requirements can be found in PCSR Chapter 30: Operation.

CB-MCR contains equipment associated with all four A-1 C&I divisions and the three A-1 electrical divisions required to support them. HMIs within the MCR include the Main Control Console (MCC), the Wide Display Panel (WDP) and the Safety Auxiliary Panel (SAuxP) for A-1 SSCs and Hardwired Backup Panels (HWBP). For functional reasons it is not possible to fully segregate SSCs from different divisions within the MCR.

The following have been identified as potential Internal Hazards within the CB-MCR [Ref-11]:

- Fire.
- Internal Flooding.
    - Immersion.
    - Spray.
- Dropped and Collapsed Load.
- Internal Missiles.
- EMI (addressed through all buildings assessment as discussed in Section 7.10)

There are no explosion sources in the CB-MCR. There are no steam release sources in the CB-MCR. There are no blast sources in the CB-MCR. There are no pipe whip or jet impact sources in the CB-MCR as all piping operates at low pressures that will not cause pipe whip or jet effects if they fail.

A comprehensive Hazard Schedule, containing all bounding hazard events identified, is presented within the Topic Report on Internal Hazards in the Main Control Room [Ref-11]. All bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.13.2 Claims and Arguments

General Claim IH_SFC_5-7.3 is considered to apply to the CB-MCR and each hazard has been assessed against to demonstrate that there is sufficient spatial and electrical separation of redundant SSCs capable of delivering the Fundamental Safety Functions.

General Claim IH_SFC_5-7.3: Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after an Internal Hazard, to fulfil the Fundamental Safety Functions.

This general claim is supported by lower level more detailed (hazard specific) claims and arguments below which together demonstrate the higher level claim has been achieved.

Claim IH_ FE_MCR_SFC_ 5-7.3: Any Design Basis Internal Fire or Explosion event originating within the MCR will not prevent delivery of the Fundamental Safety Functions

(IH_FE_MCR_SFC_5-7.3.A1 & IH_FE_MCR_SFC_5-7.3.A2)
Quantities of flammable materials in the MCR are minimised as far as is reasonably practicable. The combustible inventory in each room within the hazard compartment CB-MCR is such that design basis fires will be accommodated by the 3 hour fire resistant divisional barriers. In addition, fires originating outside of the hazard compartment CB-MCR do not propagate into the hazard compartment due to the 3 hour fire resistant barriers.

(IH_FE_MCR_SFC_5-7.3.A3)
Suitable and sufficient SSCs are located outside of the hazard compartment CB-MCR to continue to deliver the FSFs following a fire in the CB-MCR.

Claim IH_ F_MCR_SFC_ 5-7.3: Any Design Basis Internal Flood event originating within the MCR will not prevent delivery of the Fundamental Safety Functions

(IH_F_MCR_SFC_5-7.3.A1)
Flood volumes within the hazard compartment CB-MCR are small and will not challenge the divisional barriers of the CB-MCR.

(IH_F_MCR_SFC_5-7.3.A2)
The CB-MCR internal Spray hazard is bound by the CB-MCR internal Immersion hazard.

(IH_F_MCR_SFC_5-7.3.A3)
Flooding in the CB-MCR can lead to a loss of only one division of the MCR HVAC and HECW systems. In each case redundant MCR HVAC and HECW systems are available.

Claim IH_D_MCR _SFC _5-7.3: Any Design Basis Dropped Load event originating within the MCR will not prevent delivery of the Fundamental Safety Functions

(IH_D_MCR_SFC_5-7.3.A1)
Lifting operations will only be performed on equipment that is already unavailable for maintenance and hence is not affected by the dropped load. The walls, penetrations, floor and ceiling are capable of withstanding a design basis Dropped Load event.

Claim IH_CM_MCR_SFC_ 5-7.3: Any Design Basis Internal Missile event originating within the MCR will not prevent delivery of the Fundamental Safety Functions

(IH_CM_MCR_SFC_5-7.3.A1)
It is conservatively assumed that all SSCs within hazard compartment CB-MCR are unavailable after an internal missiles event. Suitable and sufficient SSCs are located outside of the hazard compartment CB-MCR to continue to deliver the FSFs following a missile impact in the CB-MCR.

7.13.3 Design Basis

The Internal Hazard assessment methodology inside the CB-MCR follows the same general approach as that for Internal Hazards outside the CB-MCR:

(1) Identify safety classified SSCs to be protected.
(2) Identify sources of Internal Hazards inside CB-MCR.
(3) Characterise the Internal Hazard, including evaluating the damage potential to SSCs.
(4) Identification of available SSCs to ensure delivery of the FSFs following an internal hazard.

Although much of the same approach for outside of CB-MCR does apply, the emphasis at each stage of the assessment differs. Within the CB-MCR segregation is not possible due to the different Class 1 divisions converging, therefore, General Claim IH_SFC_5-7.2 cannot be applied. Protection against Internal Hazards is based upon separation and/or qualification of SSCs against any relevant Internal Hazards to support safety claim IH_SFC_5-7.3. This is summarised as follows:

- **Hazard prevention:** Examples in the CB-MCR include the use of low combustibility/low ignitability/low smoke cabling, overspeed protection for rotating plant, operator training on the use of lifting equipment.
- **Spatial separation of redundant SSCs**: Examples in the CB-MCR include the separation of A-1 equipment from flood sources by weirs and internal walls, segregation of redundant HVAC equipment, where practicable separation of electrical cabling raceways to prevent fire spread between multiple divisions of SSCs.
- **Engineered Measures**: Examples in the CB-MCR include provision of Class 1 barrier to prevent hazards spreading into or out of CB-MCR, provision of alternate means of providing safety functions supported by SSCs in MCR, qualification of electrical equipment against Electro Magnetic Interference (EMI), provision of fire detection and alarm and

manual firefighting equipment, provision of dedicated MCR HVAC that ensures habitability of MCR in design basis events.

- **Administrative Measures**: Examples in the CB-MCR include maintaining 24hr occupation of the MCR in order to ensure the early detection of fires, training of operators in firefighting techniques.
- **Risk reduction measures**: Examples in the CB-MCR include casing and housing around motors and rotating plant to contain oil fires and internal missiles and the wrapping of or embedding into concrete of cables to protect from fire.

7.13.4 Safety Evaluation

7.13.4.1 Fire and Explosion inside the CB-MCR

It is expected that a fire originating inside the CB-MCR will be detected quickly and manual intervention is expected to be sufficient to extinguish it, allowing continued occupation of the MCR in line with the defend in place strategy. If the small incipient fire were to grow, the reactor would be scrammed and the MCR would be evacuated. See PCSR Chapter 21: Human-Machine Interface, for further details on MCR evacuation and PCSR Chapter 27: Human Factors, for further details on the Human Based Safety Claims associated with fire response and evacuation.

A conservative fire and explosion hazard assessment has been performed in which the fire and explosion hazard potential in each room within the hazard compartment CB-MCR has been determined [Ref-11]. There are no explosive materials identified within the CB-MCR and the total combustible inventory is such that any design basis fire will be less than 3 hours.

For the purposes of the assessment it is assumed that a fire event in hazard compartment CB-MCR could spread to all other rooms within the same hazard compartment that is not separated by the Class 1 barriers. All SSCs in the affected hazard compartment (the MCC, WDP, and MCR HVAC Systems) are conservatively assumed to fail.

As described in Section 7.4 (Internal Fire and Explosion), the Class 1 barriers of the CB-MCR, and their associated penetrations, are fully substantiated within the Barrier Substantiation Report [Ref-34] to contain the effects of a 3 hour fire to the division of origin. In addition, fires originating outside of the hazard compartment CB-MCR do not propagate into the hazard compartment due to the 3 hour fire resistant barriers.

[Ref-11] identifies suitable and sufficient SSCs located outside of the hazard compartment CB-MCR to continue to deliver the FSFs following a fire in the CB-MCR. These are described in more detail in Section 7.13.4.5 below.

7.13.4.2 Flooding Inside the CB-MCR

The flooding (immersion, spray and steam) hazard potential in each room within the hazard compartment CB-MCR has been determined in [Ref-11]. There are no steam sources within the CB-MCR and the largest flood source is associated with the HECW system pipework (other flood

sources are insignificant). There are two HECW systems HECW (A) and HECW(B) that are associated with the two independent MCR HVAC systems MCR HVAC (A) and MCR HVAC (B).

[Ref-11] demonstrates that a flooding event from either HECW system could lead to the loss of the associated MCR HVAC system but cannot affect any of the systems located within the MCR or the independent MCR HVAC system. As such, flooding event in hazard compartment CB-MCR will not affect the delivery of associated FSFs.

7.13.4.3 Dropped Loads inside the CB-MCR

The only potential dropped load hazards are associated with lifting operations of the MCR HVAC supply fans that will only take place during outage operations. The drop of the supply fan motor unit onto associated equipment within the room will not affect delivery of the associated FSFs since the specific division of the MCR HVAC System is not available due to maintenance.

The effect of a dropped load will be contained within hazard compartment CB-MCR by the robust divisional barriers that have been fully substantiated within the Barrier Substantiation Report [Ref-34] against the impact of a dropped MCR HVAC supply fan without perforation or scabbing.

7.13.4.4 Missiles inside the CB-MCR

The only internal missile sources present in hazard compartment CB-MCR are rotating components of the MCR HVAC Systems. It is likely that the spatial separation measures implemented by building design will allow the MCC, WDP and HVAC system that is not the missile source to remain available. However, it is conservatively assumed that all SSCs within hazard compartment CB-MCR are unavailable after an internal missiles event originated from the MCR HVAC Systems.

[Ref-11] identifies suitable and sufficient SSCs located outside of the hazard compartment CB-MCR to continue to deliver the FSFs following a fire in the CB-MCR. These are described in more detail in Section 7.13.4.5 below.

The effects of a missile will be contained within hazard compartment CB-MCR by the robust divisional barriers that have been fully substantiated within the Barrier Substantiation Report [Ref-34] against the impact of an MCR HVAC missile without perforation or scabbing.

7.13.4.5 Impact on A-1 SSCs within the CB-MCR

Internal Hazards within the CB-MCR will not challenge the delivery of the FSFs as suitable and sufficient A-1 and A-2 SSCs, automatic and/or manually actuated, will remain available in areas outside CB-MCR, and the delivery of the FSFs will not be affected. These alternative systems are segregated from CB-MCR with a Class 1 barrier and can be summarised as follows:

- Div. I, II, III and IV of SSLC Panels (A-1) located on Floor 1F of the CB. This automatic control system is the primary means of actuation for A-1 safety systems in the UK ABWR [Ref-29].

- Div. I and II of the RSS (A-1) located in the R/B. RSS contains the necessary monitoring and actuation equipment required to bring the reactor from hot to cold shutdown. The RSS is the claimed backup system for the SSCs primarily controlled manually from the MCR.
- Div. I and II of the Class 2 Control Panels for automatic actuation of SLC, ARI, ATWS-RPT and Feedwater Stops are located in the C/B outside the MCR and separated from the MCR by Class 1 Barriers. Additionally, Class 2 Manual Control Panels for Severe Accident (SA) C&I and the HWBS are located in the Backup Building (B/B). SA C&I shares some SSCs with the HWBS which provide actuation and monitoring of A-2 SSCs, such as FLSS, RDCF, and Containment Venting.

There will be no changes to hazard compartmentation during outage in the CB-MCR. While some potential hazards only occur in outage (e.g. dropped loads), the safety measures in place have been shown to be suitable and sufficient for all modes of operation.

7.13.5 Consequential Hazards

An assessment of consequential hazards within the CB-MCR resulting from each primary hazard has been performed in [Ref-11]. In each instance either no significant consequential hazard can occur, or the consequential hazard does not affect the SSCs outside of the CB-MCR claimed in Section 7.13.4 above.

7.13.6 ALARP Discussion

The MCR is an area of exception to segregation due to the human factors requirements for a location from which to monitor the entire plant, this means HMIs are therefore required to be linked to the C&I for multiple divisions of primary (A-1) and backup (A-2) safety systems. There is therefore no reasonably practicable way to maintain divisional compartmentation within the MCR. However, all reasonable steps have been taken to limit the likelihood of Internal Hazard occurrence and to physically separate and protect A-1 and A-2 SSCs within the compartment, for example the MCR HVAC divisions are located on different floors and cables are run in divisionalised raceways that are physically separated and have dedicated penetrations. Where practicable, the cables are provided with fire protective wrapping or embedded within reinforced concrete. This approach is in-line with UK and international good practice (such as the IAEA guidelines [Ref-26] and [Ref-27]).

In the unlikely event of an Internal Hazard event occurring within CB-MCR, measures will be in place to limit the severity of the hazard, including early detection of fires and operators trained to tackle fires at an early stage of development. The majority of hazards will be dealt with by trained MCR operators and habitation of the MCR will continue. If there is escalation of the hazard, the MCR operators will initiate manual emergency shutdown, referred to as “manual scram”, before evacuating the MCR and moving to the RSS to ensure cold shutdown is achieved. In the worst case where an Internal Hazard during any mode of operation causes evacuation of the MCR without manual scram, the bounding consequence is the failure of all SSCs in CB-MCR. See PCSR Chapter 21: Human Machine Interface, for further details on MCR evacuation and PCSR Chapter 27: Human Factors, for further details on the Human Based Safety Claims associated with fire response and evacuation.

This will not challenge the delivery of the FSFs as suitable and sufficient A-1 and A-2 SSCs, automatic and/or manually actuated, will remain available in areas outside CB-MCR, and the delivery of the FSFs will not be affected. These alternative systems are segregated from CB-MCR with a Class 1 non-divisional barrier.

It is concluded that the CB-MCR layout and design generally meets relevant good practice to either prevent internal hazard sources or effectively mitigate their consequences such that risks are ALARP.

7.13.7 Conclusions

The UK ABWR design includes many design features and operational controls to limit the sources of Internal Hazards in the MCR (and the compartment CB-MCR), reduce the frequency of hazards occurring, and limit the severity and impacts on equipment from those hazards. The design also provides adequate segregation for the redundant and diverse equipment required to maintain the Fundamental Safety Functions in the case of an Internal Hazard in the CB-MCR.

7.14 Main Steam Tunnel Room (MSTR)

7.14.1 Introduction

The Topic Report on Internal Hazards in the Main Steam Tunnel Room [Ref-12] considers the internal hazards that could affect exception to segregation SSCs located within the MSTR.

The MSTR connects the Reactor Building (R/B) to the Turbine Building (T/B) via the C/B. Divisional walls segregate the MSTR from all other rooms in the R/B, C/B and T/B, with a blowout panel within the boundary wall between the R/B and C/B portion of the MSTR and between the T/B portion of the MSTR and the T/B. The blowout panels provide pressure relief in the event of a steam release hazard and maintain containment integrity for other internal hazards.

The MSTR contains four Main Steam (MS) lines between the Primary Containment Vessel (PCV) and main steam turbine, as well as the two return Feedwater (FDW) lines from the main condenser. Each of the four MS lines have a Main Steam Isolation Valve (MSIV) inboard (i.e. within the PCV) and outboard (i.e. within the MSTR) that can isolate the MS lines at the PCV boundary. Each of the FDW lines has inboard and outboard check valves that can isolate the FDW line at the PCV boundary. The FDW lines have connections to Division A of the Residual Heat Removal System (RHR), Reactor Core Isolation Cooling System (RCIC), Reactor Water Clean-up System (CUW) and Flooding System of Specific Safety Facility (FLSS) all within the MSTR.

As discussed in Section 7.3.1.9 there is no divisional segregation within the MSTR; specifically the atmospheric temperature sensors for all 4 C&I divisions are within the same area, whilst the Main Steam Line Isolation Valves (Outboard) are associated with C&I divisions I and II. This cannot be avoided for functional reasons and therefore a different assessment approach has been applied to demonstrate that Internal Hazards within the design basis will not prevent the delivery of the Fundamental Safety Functions [Ref-12].

For the MSTR, the following hazards are included in the design basis assessment [Ref-15]:

- Fire and Explosion.
- Internal Flooding.
    - Immersion.
    - Spray.
    - Steam.
- Pipe Whip and Jet.
- Dropped Load
- Internal Missiles.
- Blast.
- EMI (addressed through all buildings assessment as discussed in Section 7.10.)

A comprehensive Hazard Schedule, containing all bounding hazard events identified, is presented within the Topic Report on Internal Hazards in the Main Steam Tunnel Room [Ref-12]. All

bounding hazard events are linked to bounding faults, as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.14.2 Claims and Arguments

General Claim IH_SFC_5-7.3 is considered to apply to the MSTR and each hazard has been assessed against it to demonstrate that there is sufficient spatial and electrical separation of redundant SSCs capable of delivering the Fundamental Safety Functions.

General Claim IH_SFC_5-7.3: Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after an Internal Hazard, to fulfil the Fundamental Safety Functions.

This general claim is supported by lower level more detailed (hazard specific) claims and arguments below which together demonstrate the higher level claim has been achieved.

Claim IH_FE_MSTR_SFC_5-7.3: Any Design Basis Internal Fire or Explosion event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

(IH_FE_MSTR_SFC_5-7.3.A1)
Quantities of flammable materials in the MSTR are minimised and controlled in accordance with COSHH and COMAH regulations. The MSTR structure is capable of withstanding the design basis fire.

(IH_FE_MSTR_SFC_5-7.3.A2)
There are no explosive materials identified within the MSTR. Any temporary quantities of explosive materials in the MSTR are minimised and controlled in accordance with COSHH and COMAH regulations. Temporary quantities of explosive materials will only be located in the MSTR during outage periods when the MS and FDW lines are isolated.

(IH_FE_MSTR_SFC_5-7.3.A3)
Whilst SSCs are assumed to be lost in the fire, the A-1 atmospheric temperature sensors within the MSTR operate on a 2 out of 4 voting logic. Any Internal Hazard which could result in loss of multiple sensors would result in an automatic signal to close the MSIVs. In addition, the inboard isolation valves are segregated by the RCCV A-1 barrier and therefore MS line isolation is still achieved.

These arguments are discussed further in Section 7.1.1.1 (Fire and Explosion inside the MSTR) below.

Claim IH_F_MSTR_SFC_5-7.3: Any Design Basis Internal Flood event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

(IH_F_MSTR_SFC_5-7.3.A1)
The walls, penetrations, floor and ceiling are capable of withstanding a design basis flood.

(IH_F_MSTR_SFC_5-7.3.A2)
The MSTR internal Spray hazard is bound by the MSTR internal Immersion hazard, and by the assumption that the entire division is unavailable upon spray release.

(IH_F_MSTR_SFC_5-7.3.A3)
The walls, penetrations, floor and ceiling are capable of withstanding a design basis steam release over-pressure. Blowout panels provide an engineered pressure release route.

(IH_F_MSTR_SFC_5-7.3.A4)
The blowout panel is a thin sheet of metal that is not capable of withstanding pressures that are a small fraction of the design basis level of the MSTR structure.

(IH_F_MSTR_SFC_5-7.3.A5)
Whilst SSCs are assumed to be lost in the flood, the A-1 atmospheric temperature sensors within the MSTR operate on a 2 out of 4 voting logic. Any Internal Hazard which could result in loss of multiple sensors would result in an automatic signal to protect the required FSFs. In addition, the inboard isolation valves are segregated by the RCCV A-1 barrier and therefore MS line isolation is still is achieved.

These arguments are discussed further in Section 7.14.4.2 (Flooding Inside the MSTR) below.

Claim IH_PJ_MSTR_SFC_5-7.3: Any Design Basis Internal Pipe Whip or Jet event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

(IH_PJ_MSTR_SFC_5-7.3.A1)
The barriers are capable of withstanding a design basis Pipe Whip event. The pipe whip cannot impact the outboard MSIVs or break safety class pipes within the MSTR.

(IH_PJ_MSTR_SFC_5-7.3.A2)
The barriers are capable of withstanding a design basis Jet Impact event. The outboard MSIVs and FDW pipework are also demonstrated to withstand the force of a direct jet impact.

(IH_PJ_MSTR_SFC_5-7.3.A3)
The A-1 atmospheric temperature sensors within the MSTR operate on a 2 out of 4 voting logic. Any Internal Hazard which could result in loss of multiple sensors would result in an automatic signal to protect the required FSFs.

These arguments are discussed further in Section 7.14.4.3 (Pipe Whip and Jet Impact inside the MSTR) below.

Claim IH_D_MSTR_SFC_5-7.3: Any Design Basis Dropped Load event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

(IH_D_MSTR_SFC_5-7.3.A1)

Lifting operations in MSTR are only carried out during outage when the Reactor is isolated. Inboard / outboard MSIVs and FDW line will be isolated. The walls, penetrations, floor and ceiling are capable of withstanding a design basis Dropped Load event.

This argument is discussed further in Section 7.14.4.4 (Dropped Loads inside the MSTR) below.

Claim IH_B_MSTR_SFC_5-7.3: Any Design Basis Blast event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

(IH_B_MSTR_SFC_5-7.3.A1)
The design basis Blast event is bounded by the Steam Release case. The walls, penetrations, floor and ceiling are capable of withstanding a design basis Internal Steam Release. Therefore, the structure of the MSTR is capable of withstanding the pressure from the design basis Internal Blast. This is discussed further in Section 7.14.4.5 (Blast inside the MSTR) below.

Claim IH_CM_MSTR_SFC_5-7.3: Any Design Basis Internal Missile event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

(IH_CM_MSTR_SFC_5-7.3.A1)
The design basis Internal Missile event is bounded by the Pipe Whip event. The walls, penetrations, floor and ceiling are capable of withstanding a design basis Pipe Whip event. Therefore, the structure of the MSTR is capable of withstanding the energy of the worst-case design basis Internal Missile. This is discussed further in Section 7.14.4.6 (Missiles inside the MSTR) below.

7.14.3 Design Basis

The Internal Hazard assessment methodology inside the MSTR follows the same general approach as that for Internal Hazards outside the MSTR:

(1) Identify safety classified SSCs to be protected.
(2) Identify sources of Internal Hazards inside MSTR.
(3) Characterise the Internal Hazard, including evaluating the damage potential to SSCs.
(4) Identification of available SSCs to ensure delivery of the FSFs following an internal hazard.

Although much of the same approach for outside of MSTR does apply, the emphasis at each stage of the assessment differs. Within the MSTR segregation is not possible due to the different Class 1 divisions converging, therefore, General Claim IH_SFC_5-7.2 cannot be applied. Protection against Internal Hazards is based upon separation and/or qualification of SSCs against any relevant Internal Hazards to support safety claim IH_SFC_5-7.3. This is summarised as follows:

- Hazard prevention.
- Spatial separation of redundant SSCs.
- Qualification of equipment.
- Engineered Measures.
- Administrative Measures.

As with the assessment of hazards inside the PCV (Section 7.12), the assessment methodologies for each Internal Hazard are similar to the equivalent methodologies outside of the MSTR. The difference to the application of the methodology is the protection against Internal Hazards is primarily focussed upon qualification of SSCs rather than segregation.

7.14.4 Safety Evaluation

The MSTR is identified as an area of exception to segregation as the hazard separation division contains instruments, components and cabling associated with SSCs from Class 1 divisions I, II, III and IV (specifically the atmospheric temperature sensors associated with all 4 Class 1 divisions and the outboard MSIVs associated with Class 1 divisions I and II).

7.14.4.1 Fire and Explosion inside the MSTR

The walls, floors and ceilings of the MSTR form a divisional barrier for fire and explosion propagation. Quantities of flammable materials in the MSTR are minimised and controlled in accordance with COSHH and COMAH regulations and [Ref-12] demonstrates that the Fire Loading inventory within the MSTR is significantly lower than other fire compartments and is significantly lower than Fire Loading inventories demonstrated not to challenge divisional barriers; as demonstrated in Section 7.4 (Internal Fire and Explosion). There is no concentration of Fire Load within the MSTR and as such it is judged that localised effects can also be discounted. In addition, there are no explosion hazards (oil mist / HEAF) identified within the MSTR.

It is recognised that temporary quantities of flammable/ explosive materials may be introduced to the MSTR during outage periods when the MS and FDW lines are isolated. Risk assessments will be in place when introducing any transient fire or explosion risks.

A fire originating in the MSTR will not propagate to other Class 1 divisions (within the T/B, R/B or C/B). The SSCs within the MSTR are assumed to be lost as a consequence of the Fire. The majority of SSCs are non-divisional or are associated with a single division (I). However atmospheric temperature sensors and the outboard MSIVs are exceptions to segregation and all divisions will be impacted by their loss.

[Ref-12] identifies suitable and sufficient SSCs located outside of the MSTR to continue to deliver the FSFs following a fire. These are described in more detail in Section 7.14.4.7 below.

7.14.4.2 Flooding Inside the MSTR

A pipe break in a Main Feedwater System (FDW) line is identified in [Ref-12] as the most onerous flood source within the MSTR. This is considered to be at any given location after the connection of the RCIC to the FDW, which would result in a release of both FDW and RCIC. Modelling within [Ref-12] shows that the source volume is sufficient to lead to flooding of all three sections of the MSTR (R/B, C/B and T/B), with excess water being released into the T/B. Any consequences within the T/B will be bound by the T/B flooding assessment in [Ref-3].

A steam line break in the MSTR would lead to a significant pressure increase in the steam tunnel leading to failure of the sacrificial blowout panels fitted at the connection of the steam tunnel to the R/B and T/B. The consequences for the SSCs within the MSTR are judged to be bounded by the immersion flooding discussed above.

[Ref-12] identifies suitable and sufficient SSCs located outside of the MSTR to continue to deliver the FSFs following an immersion or steam release. These are described in more detail in Section 7.14.4.7 below.

7.14.4.3 Pipe Whip and Jet Impact inside the MSTR

The MS lines and FDW lines within the MSTR have been identified as credible sources of pipe whip and jet. Pipe whip and jet impact analysis in [Ref-12] has shown that the divisional structures (walls, floors and ceilings of the MSTR are not breached by the pipe whip or jet impact.).

The pipework is designed such that a single pipe failure does not lead to a full bore break of any additional pipes through impact. The MS lines will not impact the FDW lines and FDW line will not impact the MS lines. Although the valve actuator of FDW line may be impacted by the MS line, the valve actuators are beyond the ECCS boundary and therefore the ECCS safety function is not affected.

Whilst the MSIVs cannot be directly impacted by the pipe whip, they will be exposed to jetting forces; [Ref-12] has shown that the MSIVs are of sufficient structural integrity that they can withstand the force of a direct jet impact on the valve stem (considered to be the weakest component of the valve).

The pipe whip assessment of FDW piping in the MSTR presented in [Ref-12] confirms that the ECCS system boundary is maintained and the ECCS function is not lost even if the jet impact between FDW main pipes occurs.

7.14.4.4 Dropped Loads inside the MSTR

The only lifting operations occur in the R/B section of the MSTR and are only carried out during outage when the Reactor is isolated. Inboard / outboard MSIVs will be closed and MS line plugs installed. The bounding lift is identified as removal of the MSIV.

A detailed analysis of the impact withstand of the MSTR is presented in [Ref-12]. This shows that the MSTR floor, walls and ceiling will contain and limit the consequences of dropped loads to the MSTR without secondary effects to adjacent divisions (i.e. no perforation or scabbing).

The lifting operation is designed so that the MSIV is not lifted over the FDW check valves. However even if the dropped load did lead to a failure of the FDW line, the check valves inside the PCV will prevent reactor water level loss and the FDW system will be shut down (note that no reactor feed pumps are operated during outage) so leakage will be negligible.

It is not possible to avoid lifting over the RHR-A line (Division I) within the MSTR, a dropped load onto this line may lead to a loss of RHR-A. Sufficient redundancy exists within the RHR to ensure that long term heat removal will continue to be delivered in the event of a loss of RHR-A.

7.14.4.5 Blast inside the MSTR

Several Blast sources have been identified for the MSTR. However [Ref-12] demonstrates that the pressure release following a steam line break bounds the effects of a blast from a pressurised device. As discussed above the MSTR is demonstrated to withstand steam release pressures (with the loss of the sacrificial blow out panels).

7.14.4.6 Missiles inside the MSTR

The Outboard MSIV Accumulators are considered to be the only missile source in the MSTR. All missile consequences from a MSIV accumulator failure event are judged to be insignificant due to the low operating pressure and are bounded by the consequences of a pipe whip. The Barrier Substantiation Report [Ref-34] demonstrates the structural capability of the MSTR barrier to limit the consequences of the postulated missile to the MSTR.

7.14.4.7 Impact on A-1 SSCs within the MSTR

The atmospheric temperature sensors identified within the MSTR are A-1 SSCs. Each of the sensors are associated with each of the four redundant electrical divisions. They operate on a 2 out of 4 voting logic therefore loss of signal to any number of the sensors due to initiating Internal Hazard or fault is acceptable. Any Internal Hazard which could result in loss of multiple sensors would result in an automatic signal to protect the required FSFs.

The MSIVs are identified as being exceptions to segregation as they are associated with Class 1 Division I and II electrical divisions although they are identified as non-divisionalised with respect to mechanical divisions. A fault or hazard occurring within a single division will not prevent closure of the MSIVs to isolate the MS lines. This configuration is not affected by a hazard occurring within the MSTR as the redundant inboard isolation valves are segregated by the RCCV A-1 barrier and therefore the function of isolation of the MS lines is achieved. It is also noted that the outboard MSIVs are normally open by retaining the pressure from MSIV accumulators to overcome the springs in the MSIV. There are two normally energized solenoid valves (supported by Division I and II electric division) to retain the pressure. De-energizing of the solenoid valves will cause

depressurization followed by MSIVs automatic closure. Loss of electricity from Class 1 Division I or II will cause the de-energizing the solenoid valve and will not prevent closure of MSIVs. Therefore a hazard occurring within the MSTR will result in the MSIVs failing to a safe isolated state.

The outboard isolation and check valves on the two return Feedwater (FDW) lines from the main condenser are non-divisionalised A-1 SSCs within the MSTR. There are redundant FDW check valves located inside the PCV that allow the FDW to be isolated in the event of a failure of the outboard isolation and check valves.

The remaining A-1 SSCs within the MSTR are associated with a single division and therefore there is sufficient redundancy external to the MSTR to continue to deliver the FSFs.

7.14.5 Consequential Hazards

An assessment of hazard combinations within the MSTR is presented in [Ref-12]. The assessment has identified that most combinations of Internal Hazard are dominated by either the primary or secondary hazard and the consequences would be no worse than the single hazard assessments discussed above. Two common initiating events (Seismic and Pressure Part Failure) have the potential to lead to multiple hazards occurring simultaneously. In each case it is argued that consequences will be no worse than assessments for the single hazards.

The potential failure of all main steam and feed lines at the point the seismic qualification changes is addressed as part of the overall seismic assessment (see PCSR Chapter 6: External Hazards).

7.14.6 ALARP Discussion

The configuration of the MSTR is such that the number of SSCs required for safety impacted by an internal hazard event is minimised to ALARP.

During the development of the GDA design an optioneering study was undertaken to analyse the MSTR in relation to the following potential design changes:

- Segregation of pipework.
- Reconsider MSTR plant layout.
- Pipe support.
- Pipework classification level.

The optioneering study is detailed in Appendix E of [Ref-12]. The outcome of the optioneering study was that MS pipework from the PCV, through the penetration into the MSTR and up to the outboard MSIVs would be VHI. The valve itself would be Standard Class 1 and designed to be ‘Fail Safe’. The pipework after the outboard MSIVs would also be Standard Class 1 transitioning to Class 3 at a defined distance away from the PCV. This is acceptable as it has been demonstrated that the

outboard MSIV has sufficient strength to withstand a Jet Impact resulting from a Pipe Break at the Class 1 to Class 3 boundary.

In addition, the existing MS pipe supports at the PCV end of the MSTR were upgraded to reduce the potential for pipe whip to occur.

The MSTR is segregated from other areas/rooms by safety divisional barriers in the form of walls, floors and ceilings which ensure that any internal hazard consequences generated within the MSTR are limited to the MSTR and FSFs can be delivered from alternative divisions. An internal hazard within the MSTR cannot impact SSCs in other rooms, areas or divisions adjacent to the MSTR.

It is concluded that the MSTR layout and design generally meets relevant good practice to either prevent internal hazard sources or effectively mitigate their consequences such that risks are ALARP.

7.14.7 Conclusions

The Internal Hazards considered above have the potential to result in SSCs from multiple Class 1 divisions to fail, however the failure modes of these SSCs are such that the Fundamental Safety Functions are not compromised by equipment failure.

In addition, Internal Hazards will such an event will not propagate beyond the MSTR such that SSCs delivering any necessary Fundamental Safety Functions in any adjacent areas, rooms or buildings are impacted.

As such Internal Hazards affecting the MSTR will not prevent delivery of the Fundamental Safety Functions and the UK ABWR will continue to operate safely following the postulated Internal Hazard events in the MSTR.

7.15 Turbine Disintegration

7.15.1 Introduction

This Section presents a summary of the Topic Report on Turbine Disintegration [Ref-13]. Internal missiles are defined as pressurised components (e.g. pipe work, valves and pressure vessels etc.) and rotating machinery (e.g. turbine-generators, diesel generators, pumps, fans, blowers, compressors, etc.) that can fail disruptively. Internal missiles may be generated when a pipe, valve or vessel disintegrates. Internal missiles may also be generated by the failure of rotating plant.

Due to the exceptional nature of the main steam turbine missile, these internal missiles are considered separately. Section 7.8 above presents a summary of [Ref-6] and considers all internal missiles other than those generated as a result of Turbine Disintegration, described as 'Conventional Missiles' whilst this Section presents a summary of the Topic Report on Turbine Disintegration [Ref-13] and considers missiles generated from the steam turbine.

The turbine disintegration hazard event is linked to a bounding fault (Fault 17.6) as identified in the Topic Report on Fault Assessment [Ref-17] and discussed in PCSR Chapter 24: Design Basis Analysis.

7.15.2 Claims and Arguments

As for all other Internal Hazards, a principal objective of the turbine disintegration safety case is to limit the effects of any design basis turbine disintegration hazard to a single division of A-1 SSCs using robust barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5 and supported by the following safety claims and arguments specific to turbine disintegration. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH_TB_SFC_5-7.1: A design basis turbine disintegration event will not result in the loss of Fundamental Safety Functions due to turbine missile impact.

Claim IH_TB_SFC_5-7.2: The frequency of turbine missile generation is minimised through good practice in plant design and operation.

This claim is supported by sub-claims IH_TB_SFC_5-7.2.1 and IH_TB_SFC_5-7.2.2 below.

Claim IH_TB_SFC_5-7.2.1: Turbine disintegration during normal operation risk is minimised through design, manufacture, inspection, testing and maintenance.

(IH_TB_SFC_5-7.2.1.A1)
The UK ABWR turbine utilises monobloc rotors which is considered to represent best practise for manufacturing high integrity turbines.

(IH_TB_SFC_5-7.2.1.A2)
Stress Corrosion Cracking (SCC) and crack expansion at the keyways on shrink fitted discs has been identified as the underlying cause of many historical turbine disintegration incidents, and this is eliminated in the adoption of monobloc rotors.

(IH_TB_SFC_5-7.2.1.A3)
A rigorous inspection and testing regime at every stage of the turbine manufacturing process ensures the reliability and integrity of the rotor, discs and blades. The fully bladed rotor undergoes extensive and rigorous overspeed tests in a vacuum chamber, at rotational speeds of 120 % of nominal. The integrity of each manufactured rotor is thus assured for overspeed events up to and above the threshold of the overspeed protection systems, minimising the potential for brittle failure due to rotor defects.

These arguments are discussed further in Section 7.15.3.5 (Prevention of Turbine Disintegration Hazards) below.

Claim IH_TB_SFC_5-7.2.2: Runaway overspeed failure risk is further minimised via the provision of a high reliability overspeed protection system.

(IH_TB_SFC_5-7.2.2.A1)
Turbine Overspeed protection is provided by three systems. Speed control during normal operation is provided by the Electro-Hydraulic Control System (EHC), which close the Turbine Control Valve and Intercept Valve following load rejection. If this system fails there are two diverse overspeed protection systems based upon mechanical and electrical principles respectively, which undergo a thorough, regular testing schedule. These ensure that turbine speeds will not exceed 112 % of nominal speed with a high degree of reliability. The frequency of turbine failure due to ductile rotor failure at runaway overspeed has been determined to be <1E-5 yr^{-1}, and is classed as a beyond design basis event.

This is discussed further in Section 7.15.3.5 (Prevention of Turbine Disintegration Hazards) below.

Claim IH_TB_SFC_5-7.3: Design basis missiles resulting from turbine disintegration do not perforate the outer structures of safety classified buildings.

This claim is supported by sub-claims IH_TB_SFC_5-7.3.1, IH_TB_SFC_5-7.3.2 and IH_TB_SFC_5-7.3.3 below. It should be noted that in the context of this claim, perforation of the T/B structure is conceded, however as the T/B is the source of the event, perforation of this structure is not considered to result in a failure to meet the claim.

Claim IH_TB_SFC_5-7.3.1: Missile ejection from the HP rotor and the generator is prevented due to retention by casing and/or stator.

(IH_TB_SFC_5-7.3.1.A1)
Assessment calculations have been performed which show that the worst credible missiles which could be generated due to fragmentation of the HP rotor will be retained by the casing of the HP turbine, and will not be ejected. Assessment of the generator rotor shows that this will not leave the stator frame if it were to fail. This is discussed further in Section 7.15.3.4 (Sources of Turbine Disintegration Hazards) below.

Claim IH_TB_SFC_5-7.3.2: All credible mechanisms by which missiles are generated from LP rotors are established. All credible missiles are classified and their characteristics are determined.

(IH_TB_SFC_5-7.3.2.A1)
Normal overspeed failure of a turbine can occur if a rotor undergoes brittle failure or stress-corrosion cracking when operating at or slightly above its nominal operating speed. Runaway overspeed failure of the LP turbine could occur if there is a loss of load to the turbo-generator, and the main steam supply fails to trip due to failure of the overspeed protection systems, causing the rotor to accelerate to speeds at which ductile rotor failure could occur.

(IH_TB_SFC_5-7.3.2.A2)
In each case, credible numbers of missiles which can be ejected are derived, together with their masses and ejection energies. Allowance is made for missile energy reduction due to the energy required to perforate the casing of the LP turbine. Sensitivity analysis have been performed within [Ref-13] on both the number of missiles generated and the significance of the LP turbine casing on the safety case.

(IH_TB_SFC_5-7.3.2.A3)
Missiles of any given ejection velocity are categorised into low trajectory and high trajectory dependent upon the path by which they could impact target structures within the site.

(IH_TB_SFC_5-7.3.2.A4)
Unmitigated fault sequences which result in frequencies of normal overspeed missile impact upon SSCs greater than 1E-7 yr^{-1} are classified as design basis, and those below this frequency as beyond design basis.

These arguments are discussed further in Section 7.15.3.4 (Sources of Turbine Disintegration Hazards) below.

Claim IH_TB_SFC_5-7.3.3: Design Basis Low Trajectory normal overspeed missiles have insufficient energy to perforate the outer structure of safety classified buildings.

(IH_TB_SFC_5-7.3.3.A1)
The buildings comprising the nuclear island are located along the axis of the turbine and away from the LP rotor ejection planes. All other buildings with a role in providing a fundamental safety function are also located away from the missile ejection planes, with the exception of the Heat Exchanger Building (Hx/B). Perforation of the T/B structure is conceded, however as the T/B is the source of the event, perforation of this structure is not considered to result in a failure to meet the claim.

(IH_TB_SFC_5-7.3.3.A2)
Damage calculations performed using the R3 impact assessment procedure demonstrate that the design basis Low Trajectory missiles ejected at normal overspeed velocities have insufficient kinetic energy to perforate the civil structure of the Heat Exchanger building (Hx/B). These missiles will result in scabbing of the civil structure and loss of a single division of the Hx/B.

(IH_TB_SFC_5-7.3.3.A3)
The LP Turbine Casing, shield walls and other structures of the Turbine Building are defence in depth measures that attenuate missile energies and reduce the extent of scabbing damage to the Hx/B civil structure.

These arguments are discussed further in Sections 7.15.3.6 and 7.15.4 below.

7.15.3 Design Basis

7.15.3.1 Turbine Disintegration Hazard Analysis Methodology

The following methodology has been applied to the assessment of turbine disintegration hazards within [Ref-13].

(1) Credible numbers of missiles which can be ejected are derived, together with their masses and ejection energies.
(2) Allowance is made for missile energy reduction due to the energy required to perforate the casing of the LP turbine.
(3) Missiles of any given ejection velocity are categorised into low trajectory and high trajectory dependent upon the path by which they could impact target structures within the site.
(4) Initiating Event Frequency and Sequence Frequency of each failure mode are estimated and beyond design basis missiles are excluded from the deterministic assessment.
(5) The barrier response to the design basis turbine missile impacts is assessed.
(6) Probabilistic assessment of the beyond design basis turbine missiles is performed.

7.15.3.2 Assessment Assumptions

The following assumptions provide the basis for assessing postulated turbine disintegration missile hazards:

- Turbine disintegration can only occur at power operation.

- In normal overspeed failure a single disc of a LP rotor is assumed to undergo brittle failure or stress-corrosion cracking.
- In normal overspeed failure, one LP disc failure will induce the failure of the two adjacent discs.
- In runaway overspeed failure, ductile rotor failure of all LP rotors is assumed to occur.
- Each LP disc is assumed to break into 3 or 4 fragments of approximately equal mass. This has been subject to a sensitivity analysis within [Ref-13] where it has been shown that breaking into 3 fragments would result in the highest kinetic energy for each fragment, whilst breaking into 4 fragments would result in the highest velocity for each fragment.
- Missiles lose energy through their interaction with the permanent features of the turbine casing and internal structures of the T/B before impacting the outer walls of the T/B. This has been subject to a sensitivity analysis within [Ref-13] where it has been shown that the turbine casing and internal structures of the T/B provide defence in depth against damage to the civil structures of the safety classified buildings.
- The LP turbine casing comprises 3 separate layers of steel and there is no disruptive failure of the casing as a result of the initial missile impact.

7.15.3.3 Design Requirement

The turbine disintegration missile claims in Section 7.15.2 has been achieved in the UK ABWR by:

- **Prevention of internal missile generation** through design and manufacturing according to appropriate international design and operational health and safety standards (see *Claim IH_TB_SFC_5-7.2.1* and Section 7.15.3.5).
- **Optimising the orientation of equipment and layout of areas** such that the number of SSCs at risk is minimised (see *Claim IH_TB_SFC_5-7.3.3* and Section 7.15.3.6)
- **Mitigating the consequences of internal missiles** through the use of suitable barriers (see *Claim IH_TB_SFC_5-7.3.3* and Section 7.15.4).

7.15.3.4 Sources of Turbine Disintegration Hazards

Normal overspeed failure of a turbine can occur if a rotor undergoes brittle failure or stress-corrosion cracking when operating at or slightly above its nominal operating speed (see *Claim IH_TB_SFC_5-7.3.2*). Runaway overspeed failure of the LP turbine could occur if there is a loss of load to the turbo-generator, and the main steam supply fails to trip due to failure of the overspeed protection systems, causing the rotor to accelerate to speeds at which ductile rotor failure could occur (see *Claim IH_TB_SFC_5-7.3.2*).

Assessment calculations have been performed in [Ref-13] which show that the worst credible missiles which could be generated due to fragmentation of the HP rotor will be retained by the casing of the HP turbine, and will not be ejected (see *Claim IH_TB_SFC_5-7.3.1*). Similarly, assessment of the generator rotor has shown that this will not leave the stator frame if it were to fail. Details of structural integrity of the HP turbine casing can be found in the Class 3 HP Turbine Casing Topic Report [Ref-35].

7.15.3.5 Prevention of Turbine Disintegration Hazards

UK ABWR includes a number of design features that prevent a missile:

- Equipment is designed and manufactured according to appropriate international design and operational health and safety standards (See Section 5.8 of this PCSR Chapter 5: Applied Regulations, Codes and Standards).
- Appropriate quality assurance programs are followed in design and fabrication.
- Commissioning, testing and inspection of equipment ensure equipment performs and continues to perform as intended.
- Turbine overspeed protection is provided.

The UK ABWR turbine utilises monobloc rotors which is considered to represent best practise for manufacturing high integrity turbines. Stress Corrosion Cracking (SCC) and crack expansion at the keyways on shrink fitted discs has been identified as the underlying cause of many historical turbine disintegration incidents, and this is eliminated in the adoption of monobloc rotors. A rigorous inspection and testing regime at every stage of the turbine manufacturing process ensures the reliability and integrity of the rotor, discs and blades. The fully bladed rotor undergoes extensive and rigorous overspeed tests in a vacuum chamber, at rotational speeds of 120Percent of nominal. The integrity of each manufactured rotor is thus assured for overspeed events up to and above the threshold of the overspeed protection systems, minimising the potential for brittle failure due to rotor defects (see *Claim IH_TB_SFC_5-7.2.1*).

Turbine overspeed protection is provided by three systems. Speed control during normal operation is provided by the Electro-Hydraulic Control System (EHC), which close the Turbine Control Valve and Intercept Valve following load rejection. If this system fails there are two diverse overspeed protection systems based upon mechanical and electrical principles respectively, which undergo a thorough, regular testing schedule. These ensure that turbine speeds will not exceed 112Percent of nominal speed with a high degree of reliability (see *Claim IH_TB_SFC_5-7.2.2*).

7.15.3.6 Protection against Turbine Disintegration Hazards

The axis of the turbine runs in a north-south direction within the turbine building. During normal powered operation of the turbine the angular momentum of each of the LP rotors is about this axis, and therefore the tangential linear velocities of the rotor components will be perpendicular to the axis. Following rotor disintegration, missiles would therefore be expected to be preferentially ejected at angles close to perpendicular to the axis. Some deflection of missiles is possible, which would result in deviations of ejection angle from the perpendicular. Those with high momenta would be unlikely to undergo significant deflection through large angles.

The buildings comprising the nuclear island are located along the axis of the turbine and away from the LP rotor ejection planes. All other buildings with a role in providing a fundamental safety function are also located away from the missile ejection planes, with the exception of the Heat Exchanger Building (Hx/B). Whilst Hx/B can be considered to be located in an ‘unfavourable’ location within the GDA site layout, Section 7.15.4, below, shows that the design basis missiles do

not cause perforation of the Hx/B structure and therefore Fundamental Safety Functions delivered by the Hx/B are not compromised. The relative location of the Hx/B with respect to the Turbine Building is discussed further in Section 7.15.5.

Ejection angles required for high trajectory missile strikes on SSCs within the GDA site layout are very close to the perpendicular. As such, there is minimal sensitivity of high trajectory missile impact probability to the location of an SSC relative to the rotor planes of rotation. All locations within the site have similar, low strike probabilities from individual high trajectory missiles. The major parameter which affects high trajectory impact probability is the plan area of the SSC. SSCs with larger areas will generally have a proportionally larger HT missile impact probability.

7.15.4 Safety Evaluation

Whilst the Topic Report on Conventional Missiles [Ref-6], makes claims on the withstand capability of barriers that are then assessed in the Internal Hazards Barrier Substantiation Report [Ref-34], the Topic Report on Turbine Disintegration [Ref-13] presents both the claims on the barriers and their substantiation through numerical analysis.

A baseline assessment has been performed of the design basis Low Trajectory missiles ejected at normal overspeed velocities. In this baseline assessment credit is taken for the LP Turbine Casing only and no credit is taken for the shield walls and other structures of the T/B. The assessment shows that the design basis missiles have insufficient kinetic energy to perforate the civil structure of the Heat Exchanger Building (Hx/B). Scabbing of the Hx/B may occur but this would result in only 1 of 3 divisions of the RCW and RSW being lost. There is sufficient divisional redundancy within the Hx/B for the RCW and RSW functions to be maintained.

A sensitivity analysis has been performed where no credit is taken for the presence of the LP Turbine Casing. This sensitivity analysis shows that, whilst the energy of impact into the Hx/B structure is significantly greater, there is no perforation of the Hx/B and only scabbing occurs.

A further sensitivity analysis has been performed where credit is taken for the LP Turbine Casing and the shield walls and other structures of the T/B. This shows that the majority of missiles would be retained within the T/B, and those that exited the building would have insufficient energy to scab the Hx/B.

It is concluded, therefore, that the LP Turbine Casing and the shield walls and structures of the T/B are defence-in-depth measures that contribute to a reduction in the extent of damage to the Hx/B from the design basis Low Trajectory normal overspeed missiles.

Assessment of the High Trajectory missiles ejected at normal overspeed velocities has shown that the impact frequency on safety significant buildings is substantially lower than 1E-7 yr^{-1} in all cases.

The frequency of turbine failure due to ductile rotor failure at runaway overspeed has been determined to <1E-5 yr^{-1}, and is classed as a beyond design basis event. The impact frequency of LT runaway overspeed turbine missiles on SSCs with a safety function is less than 1E-7 yr^{-1} in most

cases. The impact frequency of HT runaway overspeed missiles is substantially lower than 1E-7 yr^{-1} in all cases.

Beyond design basis sequences which result in the loss of the principal means of delivering fuel cooling and long-term heat removal functions are mitigated by provision of sufficient diverse systems to ensure continued delivery of the functions. For instance, complete loss of the Hx/B, which houses portions of each of the three trains of RCW and RSW systems is mitigated by the RCIC and FLSS systems. In the event of complete failure of the ECCS, FLSS and FLSR systems can be deployed to ensure fuel cooling and long-term heat removal (See Section 13.4 in PCSR Chapter 13 and 16.7 in PCSR Chapter 16).

7.15.5 ALARP Discussion

The risk of a disruptive turbine failure event giving rise to rotor disintegration and ejection of high energy missiles is minimised by the adoption of a high reliability turbine design, high quality manufacturing processes, rigorous inspection and factory testing. During operation, monitoring systems and diverse lines of overspeed protection further reduce the risk of rotor failure.

The layout of the ABWR site is optimised with respect to the turbine disintegration hazard, and takes account of the tendency for turbine missiles to be preferentially ejected close to the planes of rotation of the rotors. Structures performing or housing FSFs are generally located as far from these regions as is practicable.

The assessment presented in [Ref-13] identifies that turbine missile risk is dominated by the Hx/B, which contains Class 1 safety systems and is located relatively close to the plane of rotation of the turbine. If the structure of the Hx/B is challenged, the layout of the three divisions of RCW/RSW equipment further reduces the risk that the FSFs performed by the Hx/B will be lost, providing additional defence in depth. If all three divisions of the Hx/B are lost due to missile impact, this fault is bounded by common cause failure of the RCW/RSW systems. In this case, diverse means of maintaining long term core cooling is provided by systems housed within the R/B and B/B.

It is therefore demonstrated that UK ABWR has a robust deterministic safety case for the turbine disintegration hazard. The assessment [Ref-13] also presents the findings of an ALARP study of potential risk reduction options for the Hx/B. The study considered a range of options including changes to plant layout, separation / segregation, redundancy, structural strengthening of buildings and other protection measures aimed at eliminating or reducing the risk

The study concluded that there is no strong risk driver for major design change; the design basis Turbine Disintegration events do not lead to a loss FSFs. A number of potential risk reduction measures are being taken forward for more detailed assessment/ review during the post GDA phase.

7.15.6 Conclusions

The UK ABWR design includes many design features and operational controls to limit the potential for turbine disintegration to occur and limit the severity and impacts on safety significant structures and systems from missiles. Design basis missiles cannot penetrate the outer structures of the safety classified buildings and will not compromise delivery of the Fundamental Safety Functions.

The design provides for redundant and diverse equipment to maintain the Fundamental Safety Functions that are separated and segregated such that any missile impact onto these systems is a beyond design basis event.

7.16 Internal Combined Hazards

7.16.1 Introduction

The Topic Report on Combined Internal Hazards [Ref-14] consideres the combinied internal hazsards that can occur within the UK ABWR site boundary and buildings. There are three distinct mechanisms in which design basis Internal Hazards may occur in combination. These are:

- **Consequential Hazards;** These are where an event causing a primary hazard also gives rise to one or more secondary hazards due to a direct causal relationship. For example, a dropped load could damage a pipe causing internal flooding.

- **Correlated Hazards;** These are multiple hazards which occur as the result of a single underlying cause. The underlying cause could be either internal or external. For example, a seismic event could cause a dropped load and pipe failure in separate locations in the plant, or failure of a pressurised pipe may result in a combination of pipe whip, internal blast, jetting, steam release, spray and/or immersion.

- **Independent Hazards;** Internal Hazards are considered to be independent if they could only be expected to occur together by random coincidence, due to there being no causal association between the initial events. The simultaneous occurrence of hazards also includes hazards that occur in succession of another fault or hazard, which may have resulted in safety related plant being degraded or compromised.

It has been assessed that the probability of simultaneous occurrence of internal hazards is so low that they can be discounted.

7.16.2 Claims

The principal means of mitigating combined hazards is through the containment of the effects of the hazard within the division of the initiating event using barrier compartmentation. This is summarised in the general claims for Internal Hazards made within section 7.3.1.5 and supported by the following safety claims with respect to combinations of Internal Hazards. Appendix A presents the full claims table for this PCSR Chapter.

Claim IH ICH_SFC 5-7.1: Combined Internal Hazards
Any combination of Internal Hazards within the design basis will not prevent the delivery of the Fundamental Safety Functions.

This claim is supported by sub-claims IH_ICH_SFC_5-7.1.1, IH_ICH_SFC_5-7.1.2 and IH_ICH_SFC_5-7.1.3 below.

Claim IH ICH_SFC 5-7.1.1: Consequential Internal Hazards

Any potential event which gives rise to a design basis Internal Hazard directly resulting in the occurrence of additional, secondary hazards is minimised in the design by measures such as segregation, separation and qualification of equipment.

(IH_ICH SFC_5-7.1.1 A1)
For buildings containing Class 1 equipment, redundant divisions of equipment are segregated by Class 1 Divisional barriers.

Claim IH_ICH_SFC 5-7.1.2: Correlated Internal Hazards
The simultaneous or successive occurrence of two or more design basis Internal Hazards with a single, underlying cause will not result in a more onerous consequences than if any of the hazards were to occur in isolation.

(IH_ICH SFC_5-7.1.2 A1 & IH_ICH SFC_5-7.1.2 A2)
Individual internal hazards identified as being related to a single event (e.g. pressure part failure) do not combine in such a way that the combined hazard loads lead to any additional safety impacts when compared to the individual single hazards. Exceptions to this argument are covered by IH ICH SFC 5-7.1.2.A2

Where loss of two A-1 divisions can occur and therefore result in more onerous consequences, the UK ABWR still meets the requirements for fault tolerance and sufficient A-1/A-2 SSCs are available to maintain the FSFs. In this way, the outcome of this assessment bounds any postulated failure of a Class 1 barrier due to combinations of internal hazards or beyond design basis single hazards.

Claim IH_ICH_SFC 5-7.1.3: Independent Internal Hazards
The simultaneous or successive occurrence of two or more design basis Internal Hazard events without any direct causal link is of sufficiently low probability that any such scenarios can be screened out on the basis of frequency.

(IH_ICH SFC_5-7.1.3 A1 & IH_ICH SFC_5-7.1.3 A2)
All independent combinations of infrequent hazards identified for the ABWR are below 10-7 /yr for recovery times of 1 month or less, and significantly below 10-5 /yr for recovery times of 1 year.

The frequency of two independent fires simultaneously damaging two redundant divisions of A1 plant is below 10-5 /yr for recovery times of less than 1 month. Increased recovery times would result in the hazard combination being infrequent, and in order for the hazard combination to be frequent the recovery time would need to be as high as 10 years. The conditional probability of a fire being severe enough to require a recovery time of greater than one month, and certainly as high as 10 years, is significantly less than 1 and would further reduce the frequency of the combination.

Claim IH_ICH_SFC 5-7.2: Limitation of consequential Internal Hazards to a single division
The divisional barriers segregating neighbouring divisions will fully accommodate the effects of relevant combined hazards generated within the room or area containing the barrier.

(IH_ICH SFC_5-7.2 A1)

Any effects from an event in one division (e.g. concrete scabbing) will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

Claim IH_ICH_SFC 5-7.3: Limitation of consequential Internal Hazards by qualification
Where divisions are not segregated by physical barriers, and hazard protection is provided by separation or local protection, combined hazards will not damage sufficient safety measures in multiple divisions to prevent the delivery of the FSFs.

(IH_ICH SFC_5-7.3 A1 & IH_ICH SFC_5-7.3 A2)
Individual internal hazards identified as being related to a single event (e.g. pressure part failure) do not combine in such a way that the combined hazard loads lead to any additional safety impacts when compared to the individual single hazards. Exceptions to this argument are covered by IH ICH SFC 5-7.3.A2

Where loss of two A-1 divisions can occur and therefore result in more onerous consequences, the UK ABWR still meets the requirements for fault tolerance and sufficient A-1/A-2 SSCs are available to maintain the FSFs. In this way, the outcome of this assessment bounds any postulated failure of a Class 1 barrier due to combinations of internal hazards or beyond design basis single hazards.

Section 7.16.4 presents a summary of the GDA assessment for a postulated design basis combined hazard event.

7.16.3 Design Basis

7.16.3.1 Combined Hazard Analysis Methodology

The combined hazard assessment has been performed based on the following approach. This methodology is consistent with Section 7.2.1 and the further detail presented in section 7.3.2:

(1) **Define combination types and assessment criteria.** The assessment criteria provide a basis for identifying foreseeable hazard combinations, and for identifying those combinations which could provide a threat to the divisional barriers and safety systems beyond that assessed within the single hazard TRs.
(2) **Identify hazard combinations requiring assessment.** The detailed results for this task are provided in the form of a screening table. The results are summarised, identifying the hazard load combinations on barriers to be taken forward for further assessment. Note that no hazard combinations are excluded from the safety case assessment.
(3) **Assess structural response of barriers to combinations taken forward.** This assessment is primarily in relation to impact of combinations on the divisional barriers.
(4) **Application of assessment to each divisional barrier.** The generic assessment is applied to all A1 Class 1 divisional barriers within the UK ABWR plant, showing where combinations have either been screened for that barrier, do not physically occur for that barrier, or the barrier will withstand the effects of any hazard load combinations on barriers.

This assessment is outlined and a barrier summary table in [Ref-14] is provided which shows how each divisional barrier responds to internal combined hazards.

(5) **Determine suitability and sufficiency of safety measures.** Confirmation is provided that the safety measures adopted for the ABWR are adequate for internal combined hazards. This conclusion is based on review of the single hazard TRs, and a further deterministic assessment that considers the potential loss of two A1 divisions in the event of a hazard damaging a divisional barrier. A hazard schedule in [Ref-14] is provided summarising the safety measures claimed against a set of fault sequence groups that encompass each internal hazard combination and plant building and operation mode.

The methodology for internal combined hazards (ICH) follows a similar approach to that applied to the assessment of combined external hazards for the UK ABWR. In order to arrive at a meaningful number of potential combination events, the assessment adopts a screening approach, based on a set of Screening Criteria, to identify a list of foreseeable combined internal hazards.

The remaining consequential and correlated hazard combinations were subject to a thorough review, this identified 15 foreseeable internal hazard combinations to be taken forward for further assessment. This includes two correlated hazard cases relating to pressure part failure. Two bounding rooms within the R/B are assessed in detail in [Ref-14].

7.16.3.2 Assessment Assumptions

The following assumptions are made for the combined hazards assessment:

- External hazards can be the source of both consequential and correlated Internal Hazards*
- Pipework is not considered as a missile source due to the high ductility, it is considered as a Pipe Whip hazard and is assessed in Section 7.6 above.
- Combinations involving industrial and EMI hazards were screened from the assessment on the basis of their low impact
- Independent combinations of hazards were not taken forward for detailed assessment. It is noted that frequency alone is not used to preclude hazards combinations and these combinations were also assessed in relation to design basis criteria in the Safety Case Development Manual (SCDM) showing that sufficient safety measures would be available in the event of the independent hazard combinations.

*External hazards are reviewed and shown not to result in consequential internal hazards.

7.16.3.3 Design Requirement

The UK ABWR design is such that the combined hazards claims in Section 7.16.2 are principally delivered by Class 1 divisional barriers segregating divisions of A-1 safety-related SSCs providing redundancy. The safety divisional barriers confine the hazard event to the division of origin such that redundant A-1 SSCs are available to deliver any required FSFs. The A-1 divisional segregation limits the consequences of the Internal Hazard event from propagating beyond the division of origin.

In addition, the following safety measures are implemented in the UK ABWR to reduce the risk from combined hazards:

- **Hazard prevention**: The likelihood of Internal Hazards occurring in the first instance is reduced or designed out where practicable. This includes limiting the potential sources and initiating events and also the likelihood of hazard escalation.

- **Compartmentation and spatial separation**: The general protection arrangement used to limit the severity of an initiating event against all internal hazard events in the UK ABWR is the divisional barrier. The divisional barrier is a Safety Class 1 passive reinforced concrete wall/floor/ceiling used in the UK ABWR to provide divisional segregation between redundant and diverse Safety Class 1 SSCs. Some safety systems are separated spatially, e.g. the EDGs are located in separate buildings. In some cases spatial separation may be claimed within divisions although in relation to exceptions to segregation.

- **Other Engineered Measures**: The risk from some internal hazards can be managed via engineered measures, other than the barriers, designed to prevent or mitigate the effects of a hazard. These include the use of good design practices such as fire detectors and dampers. Suppression is provided in some areas to reduce the consequences of internal fires that break out. The casing of rotating machinery prevents the breaching of missiles.

- **Administrative Measures**: The risk from some Internal Hazards can be reduced via administrative controls which include operator procedures and training. The detail of how administrative controls will be implemented will be the responsibility of the future licensee.

- **Risk reduction measures**: In addition, the non-divisional walls / floors / ceilings also provide defence in depth protection arrangements against propagation of initiating events. Although these walls/floors/ceilings are not Safety Class 1 SSCs, the robust design of these civil structure provides an inherent level of hazard containment. These civil structures are constructed of reinforced concrete, which has good structural integrity, and fire, flooding, and impact resistances.

7.16.3.4 Sources of Combined Hazards

The individual Internal Hazards identified as requiring combined hazards assessment are Fire and Explosion, Flood (encompassing; Immersion, Spray and Steam Release), Pipe Whip, Conventional Missile, Blast, and Dropped Load. As discussed above, there are no consequential or correlated effects relating to the Internal EMI Hazards.

Potential combinations (Consequential and Correlated) involving the Internal Hazard sources above have been determined for each assessment area.

It has also been identified that there is a potential for a Design Basis Seismic Event to initiate an Internal Hazard within the buildings (e.g. post seismic fire and or flooding).

7.16.4 Safety Evaluation

7.16.4.1 General Approach to Combined Hazards Consequences

Where combined hazards are assumed to occur the combined hazard analysis conservatively assumes that all SSCs in the division of origin are lost during the hazard. In addition, it assesses the divisional barrier walls, ceilings and floors to determine whether divisional segregation is compromised by the combined hazard and equipment in other divisions is also compromised.

There are a number of known exceptions to segregation where it is not reasonably practicable to divide these areas with barriers; the PCV, the MCR and the Main Steam Tunnel Room, these have been subject to specific Internal Hazards assessments in Sections 7.12, 7.13 and 7.14 respectively.

There are other areas where it may be justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment; such A-1 or A-2 SSCs are referred to as exceptions to segregation SSCs. Where these exceptions to segregation exist, it has been demonstrated in [Ref-25] that the FSFs can still be delivered following an internal hazard that affects such exceptions to segregation SSCs.

7.16.4.2 Consequences of Combined Hazards at Power

A number of the potential consequences for combinations identified cannot be formally assessed due to the lack of detail within the current design and will required to be assessed during the detailed design phase. During this stage more information associated with the assessment will be available to enable a better understanding of the range of influence individual hazards may have. For example, detailed piping routes are currently not available until the detailed assessment stage and therefore the Pipe Whip hazard (and the consequential affects from such) can be identified but cannot be assessed to the full extent of potential interactions.

Whilst detailed analysis of all hazard combinations cannot be completed at this time, it is anticipated that an Internal Combined Hazard event (not due to a seismic event) during power operation can be demonstrated to only result in loss of a single division of safety classified A-1 SSCs. Bounding assessments for divisional barrier response to secondary hazards caused by a pressure part failure have been undertaken, which demonstrates that the barrier will not be compromised. This provides confidence that credible combined hazards are likely to be confined to the division of origin. Furthermore, detailed assessment of the availability of SSCs to deliver FSFs for hazard leading to the loss of two A-1 division has been performed [Ref-14].

For a seismic event, the Fault Schedule [Ref-17] identifies the equipment required to respond to a frequent (10^{-3}) earthquake and Design Basis Earthquake (DBE) event and identifies the most limiting collection of equipment to fulfil the FSFs for all operational modes (at power and during an outage). It is anticipated that the resultant Internal Combined Hazard events will not result in the loss safety classified A-1 SSCs required to deliver the FSFs. The principal safeguard to prevent multiple fire initiation in different divisions is to seismically qualify relevant equipment that could contribute to fire initiation.

7.16.4.3 Consequences of Combined Hazards during outage

As the detailed outage schedule will be provided by the future licensee at site specific stage, it has been necessary to make a set of highly conservative assumptions as part of the outage deterministic assessment. In particular, where hatches are required to be open to allow movement of equipment, these are assumed open during that phase of the outage. Some hatches pass through multiple divisions. This reduces the extent of divisional compartmentation provided between A-1 SSCs of different divisions in some stages of outage.

However, assessments of available systems in outage show that there remain suitable and sufficient A-1 and A-2 SSCs during an Internal Hazard in any phase of outage to deliver the FSFs, this includes the Class 2 FLSS, Class 2 HWBS. In addition, a range of Class 3 systems including FLSR, MUWC and SPCU are also available.

7.16.5 Conclusions

Whilst detailed analysis of hazard combinations cannot be completed at this time, it is anticipated that an Internal Combined Hazards event will not affect SSCs required for safety and that redundant systems remain available to ensure the delivery of the Fundamental Safety Functions. Therefore, it is anticipated that the nuclear safety risks of the design will be demonstrated to be tolerable and ALARP.

7.17 Assumptions, Limits and Conditions for Operation (LCO)

7.17.1 Assumptions for Internal Hazards

This Chapter presents a summary of the detailed Internal Hazards assessments that have been performed in support of the PCSR. Sub-Section 7.x.3.2 of Sections 7.4 (Internal Fire and Explosion) to 7.16 (Internal Combined Hazards) above present the specific assumptions used in each assessment.

7.17.2 Limits and Conditions of Operation

One purpose of this generic PCSR is to identify constraints that must be applied by a future licensee of a UK ABWR plant to ensure safety during normal operation, fault and accident conditions. Some of these constraints are maximum or minimum limits on the values of system parameters, such as pressure or temperature, whilst others are conditional, such as prohibiting certain operational states or requiring a minimum level of availability of specified equipment. They are collectively described in this PCSR as Limits and Conditions for Operation (LCOs).

LCOs applicable to design basis analysis fall into a number of categories:

- LCOs that define the initial conditions of faults
- LCOs that guarantee the delivery of Safety Functions
- LCOs that maintain accident doses within limits

The Internal Hazards assessment discussed in this Chapter supports the design basis analysis by assessing:

- How design basis Internal Hazards affect SSCs in the UK ABWR,
- How loss of those SSCs might impact the ability to deliver the High Level Safety Functions/ Fundamental Safety Functions,
- What safety measures are required such that there are always suitable and sufficient A-1 and/or A-2 SSCs remaining following any Internal Hazard (or combination of hazards) to deliver the Fundamental Safety Functions.

The Internal Hazards assessment, therefore, only considers LCOs that guarantee delivery of Safety Functions.

7.17.3 LCOs that guarantee the delivery of Safety Functions

The Design Basis assessment assumes the availability of a certain number of safety systems, usually one division of each system. The analysis also assumes single failures, again usually of one division of each system. These assumptions lead to Safety Property Claims (SPCs) derived from the NSEDPs [Ref-32] and summarised in PCSR Chapter 5 section 5.3 that Class 1 systems have N+2 redundancy and Class 2 systems have N+1 redundancy.

The Internal Hazards assessment has shown how, at power operation and during outage, divisional segregation, equipment qualification and fail safe operation of the Class 1 and Class 2 systems supports the system redundancy SPCs. It should be noted that the Internal Hazards assessment does not introduce any new SPCs, these are presented in the PCSR Chapters describing SSCs required for safety (see Appendix B for further details).

The Internal Hazards assessment has highlighted that this required availability for safety systems will place constraints on which systems may be maintained during operation, what action must be taken in what timescale if a system is discovered to be in a failed or degraded state during surveillance testing and what systems can be removed concurrently for maintenance during planned outages.

The specific details of the LCOs is outside the scope of this Chapter, however, these factors will lead to LCOs being defined to ensure the required availability of Class 1 and Class 2 systems.

7.18 Summary of ALARP Justification

7.18.1 Introduction

This Section presents a high level overview of how the ALARP principle has been applied for Internal Hazards, and how this contributes to the overall ALARP argument for the UK ABWR.

In summary, it is concluded that all reasonably practicable risk reduction measures have been implemented, through the application UK and international good practice and a systematic and comprehensive ALARP evaluation process. The risks due to Internal Hazards are therefore considered to be ALARP.

7.18.2 ALARP Discussion

PCSR Chapter 28 presents an overview of how the UK ABWR design has evolved, and how this evolution contributes to the overall ALARP case. The approach to ALARP during GDA is further described in the GDA ALARP Methodology [Ref-22]. For the mechanical systems covered by this Chapter, this ALARP methodology has also been embedded within the design process [Ref-41]. This places requirements on designers to consider ALARP through a comprehensive checklist which includes such elements as optioneering, risk assessment and the identification of RGP and OPEX.

For Internal Hazards, specific areas where Relevant Good Practice (RGP) has been identified and applied include:

- Lifting operations are designed such that, where reasonable practicable, the lifts performed will remain within the Class 1 division of origin. The lifting routes will utilise hatches immediately above the division of equipment and transfer routes designed to ensure that the lift remains within the Class 1 division of origin, where possible.
- The Main Steam Tunnel Room (MSTR) links the Reactor Building (R/B) to the Turbine Building (T/B), and contains the main steam lines and the Feedwater lines. A failure of one of these high energy pipe lines could lead to pipe whip which could damage other lines, potentially leading to a ‘domino’ effect and multiple pipe failures. Internal Hazards assessment has concluded that this domino effect will not occur within the design basis due to pipe integrity and even if it did occur the ECCS function (part of the Fundamental Safety Functions in the MSTR) will not be compromised. Furthermore, piping support has been enhanced to restrain any pipe whip as a defence in depth measure. Further detail can be found in a Topic Report on Main Steam Tunnel Room [Ref-12].
- The reference design included a number of penetrations in the Class 1 barriers between Class 1 divisions that were closed by single doors. This introduced a potential vulnerability, if the door is not closed when a demand is placed on the barrier. Practice in Japan is that operational controls are adequate to address this risk, however to bring the design in line with UK good practice, Hitachi-GE carried out an ALARP review of all doors in Class 1 barriers. The aim of this review was to minimise the number of doors in Class 1 barriers, and where the door could not reasonably be removed, implement a double door and lobby

arrangement. Where double doors were concluded not to be reasonably practicable, single doors would be used, but fitted with alarms that annunciate both locally and in the Main Control Room (MCR) if the door is left open. Further details can be found in a Topic Report of Doors on Class 1 Barriers [Ref-16].

- Bunding will be added around large oil tanks to collect leaks and limit the size of any pool fires.
- Spray guards will be used to prevent oil mist hazards.
- Switchgear will be designed to UK standards (e.g. BS EN 62271-200) to minimise the potential for High Energy Arcing Faults.

For Internal Hazards, specific examples of where ALARP assessments have been used to inform the design include:

- The reference design for the Emergency Diesel Generators (EDGs) followed Japanese practice of locating the EDGs within the Reactor Building (R/B). While this offers advantages in terms of seismic withstand and aircraft impact resistance, the potential fire risk due to large fuel tanks being located inside the R/B prompted the search for potential risk reduction measures. Relocation of the EDGs was extensively optioneered by a multi-disciplinary team, taking into account such factors as internal and external hazards, overall nuclear safety, reliability, maintainability and constructability. This has resulted in a design change whereby the EDGs will be segregated both from each other (there are three redundant EDGs each capable of supplying all the plant's Emergency power) and from other primary and backup safety systems (A-1 and A-2 SSCs) by locating each EDG in its own dedicated building physically separated from the main UK ABWR buildings. Further detail is presented in a Topic Report on EDG Relocation [Ref-24].
- Full assessment of radiolytic gases in UK ABWR process and plant led to following design changes:
    a. Changes to piping gradients, piping diameters and addition of venting lines to prevent accumulation of radiolytic gases (particularly in the T/B).
    b. Adoption of new "flat-top" RPV water level and pressure monitor and MSL flow monitor condensing chambers to reduce volume of hydrogen that can accumulate with the instrument. For the MSL flow monitors, the piping gradient was also changed to downward sloping to eliminate risk of any accumulation.
- The outage maintenance schedule has been revised so that at worst one division of A-1 and one division of A-2 SSCs will be simultaneously offline for maintenance, earlier iterations of the outage schedule had up to divisions of A-1 SSCs in maintenance at the same time.
- The piping route for the hydrogen generator cooling systems in the T/B has been optimised to limit the potential for hydrogen explosions to damage important equipment.
- Assessment of the loads on divisional barriers in [Ref-34] has identified a number of increases in barrier thickness/ reinforcement to ensure that the barriers achieve the required performance. These modifications to the barriers will be carried forward to the detailed design phase.

7.18.3 Conclusions

Further discussion on ALARP is included within each of the Topic Reports that support this Chapter. Each of the BSCs that cover SSCs that contribute to the Internal Hazards safety case also contains a section which discusses RGP and OPEX.

7.19 Overall Conclusions

This PCSR Chapter presents the assessment of Internal Hazards for the UK ABWR. The following hazards have been assessed both individually and in combination:

- Internal fire and internally initiated Explosions.
- Internal flooding including.
  - Immersion.
  - Spray.
  - Steam Release.
- Pipe whip and liquid jet impact.
- Dropped loads and collapsed loads.
- Internally generated missiles.
  - Conventional missiles.
  - Turbine Disintegration.
- Blast effects (non-combustible effects e.g. blast following pressure part failure).
- Internally generated Electromagnetic Interference (EMI) and internally generated Radio Frequency Interference (RFI).
- Miscellaneous Hazards.
  - On-site hazardous materials including.
  - On-site transportation accidents.
  - Pipeline accidents.
  - Natural gases from the ground (e.g. methane).

With respect to hazards protection, the design of the UK ABWR is primarily based on providing redundant and diverse safety systems segregated by robust barriers (divisional barriers) which contain an Internal Hazard within the affected division and prevent the spread of the hazard to a different division. The robust UK ABWR design also includes measures and systems designed to prevent Internal Hazards occurring. These preventative systems and procedures provide “defence in depth” against the loss of equipment that delivers a Fundamental Safety Function.

The assessment of Internal Hazards has analysed the robustness of these divisional barriers against design basis Internal Hazard events (individually and in combination) and has shown that in the majority of cases that the divisional barriers are capable of resisting the potential Internal Hazard (or combination of hazards) and that sufficient redundancy and diversity of safety systems is assured in all operational states to ensure delivery of the Fundamental Safety Functions.

For some hazards, the assessment is limited by there being no detailed layout, which forces an assessment based on a set of highly conservative assumptions about Internal Hazard and nature of the impacts. In a small number of cases, this highly conservative analysis has predicted a degree of damage to the divisional barriers. Further analysis has shown that reasonably practicable modifications can be implemented during detailed design that will either eliminate or reduce the magnitude of the hazard such that barriers will demonstrably resist the potential Internal Hazard (or combination of hazards).

In a small number of instances it is neither practicable nor desirable to implement divisional separation of safety systems. In particular, it may be justifiable and ALARP to have A-1 SSCs from more than one division or both A-1 and A-2 SSCs in the same hazard compartment; such A-1 or A-2 SSCs are referred to as exceptions to segregation. An assessment of the impact of a loss of exceptions to segregation SSCs has shown that, in all cases, this will not challenge the delivery of the Fundamental Safety Functions as suitable and sufficient A-1 and A-2 SSCs, automatic and/or manually actuated, will remain available in areas segregated from the hazard affected zone.

With respect to Internal Hazards, the UK ABWR has adopted Relevant Good Practice including the enhancements to piping support in the Main Steam Tunnel Room (MSTR) and the use of two sets of doors where possible to facilitate access through divisional boundaries. Furthermore, ALARP assessments have been used to inform the relocation of Emergency Diesel Generators and changes to the proposed outage schedule to ensure that sufficient safety systems are available in all operational modes.

In summary, it is concluded that all reasonably practicable risk reduction measures have been implemented, through the application UK and international good practice and a systematic and comprehensive ALARP evaluation process. The risks due to Internal Hazards are therefore considered to be ALARP.

7.20 References

[Ref-1] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Approach to Internal Hazards", GA91-9201-0001-00085 (SE-GD-0192), Rev.1, Febuary 2017.

[Ref-2] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Fire and Explosion", GA91-9201-0001-00090 (BKE-GD-0018), Rev.5, March 2017.

[Ref-3] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Internal Flooding", GA91-9201-0001-00091 (SE-GD-0143), Rev .4, June 2017.

[Ref-4] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Pipe Whip and Jet Impact", GA91-9201-0001-00092 (ZD-GD-0008), Rev.5, June 2017.

[Ref-5] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Dropped and Collapsed Loads", GA91-9201-0001-00093 (LE-GD-0082), Rev.4, July 2017.

[Ref-6] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Internal Missile – Conventional Internal Missiles", GA91-9201-0001-00181 (SE-GD-0346), Rev 5, June 2017.

[Ref-7] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Internal Blast", GA91-9201-0001-00095 (SE-GD-0199), Rev 4, June 2017.

[Ref-8] Hitachi-GE Nuclear Energy, Ltd., "Topic Report of Electro Magnetic Interference", GA91-9201-0003-00083 (3E-GD-A0096), Rev 4, June 2017.

[Ref-9] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Miscellaneous Internal Hazards", GA91-9201-0001-00097 (SE-GD-0218), Rev 2, March 2017.

[Ref-10] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Internal Hazards in the Primary Containment Vessel", GA91-9201-0001-00131 (SE-GD-0268), Rev 3, Febuary 2017.

[Ref-11] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Internal Hazards in the Main Control Room", GA91-9201-0001-00185 (SE-GD-0355), Rev 1, December 2016.

[Ref-12] Hitachi-GE Nuclear Energy Ltd, "Topic Report on Internal Hazards in Main Steam Tunnel Room", GA91-9201-0001-0098 (SE-GD-0232) Rev.3, March 2017.

[Ref-13] Hitachi-GE Nuclear Energy Ltd., "Topic Report on Turbine Disintegration Safety Case", GA91-9201-0001-00260 (AE-GD-0959) Rev.1, July 2017.

[Ref-14] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Combined Internal Hazards", GA91-9201-0001-00096 (SE-GD-0217), Rev.4, August 2017.

[Ref-15] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Internal Hazard Identification", GA91-9201-0001-00086 (SE-GD-0193), Rev.0, November 2014.

[Ref-16] Hitachi-GE Nuclear Energy Ltd., "Topic Report of Doors on Class 1 Barriers", GA-91-9201-0001-0099 (SE-GD-0190) Rev.3, November 2016.

[Ref-17] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Fault Assessment" GA91-9201-0001-00022 (UE-GD-0071), Rev.6, July 2017.

[Ref-18] Hitachi GE Nuclear Energy, Ltd., "Topic Report on Safe Management of Radiolytic Gases Generated During Normal Operations", GA91-9201-0001-00129 (SE-GD-0250), Rev.4, June 2017 .

[Ref-19] IAEA, "Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants", No. NS-G-1.7, 2004.

[Ref-20] US NRC Standard Review Plan, BTP 3-3 "Protection Against Postulated Failures in Fluid Systems Outside Containment", Rev.3, March 2007.

[Ref-21] Health and Safety Executive "Control of Major Accident Hazards (COMAH) Regulations", 2015.

[Ref-22] Hitachi-GE Nuclear Energy Ltd., "GDA ALARP Methodology", GA10-0511-0004-00001 (XD-GD-0037) Rev.1, November 2015.

[Ref-23] Hitachi-GE Nuclear Energy Ltd., "General Design Process Approach for Mechanical Engineering SSCs", GA91-9201-0003-00854 (SE-GD-0297) Rev.1, September 2016.

[Ref-24] Hitachi-GE Nuclear Energy Ltd., "Topic Report of the Emergency Diesel Generator Locations Optioneering Study", GA91-9201-0001-00170 (LE-GD-0192) Rev.0, December 2015.

[Ref-25] Hitachi-GE Nuclear Energy Ltd., "Topic Report on Exceptions to Segregation", GA91-9201-0001-00084 (BKE-GD-0021) Rev.3, April 2017.

[Ref-26] International Atomic Energy Agency, "Preparation of Fire Hazard Analyses for Nuclear Power Plants", Safety Reports Series No. 8, 1998.

[Ref-27] International Atomic Energy Agency, "Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants Safety Guide", IAEA Safety Standards Series NS-G-1.7, 2004.

[Ref-28] International Atomic Energy Agency, "Protection against Internal Hazards other than Fire and Explosions in the Design of Nuclear Power Plants Safety Guide", IAEA Safety Standards Series NS-G-1.11, 2004.

[Ref-29] Hitachi-GE Nuclear Energy Ltd., "Basis of Safety Cases on Safety System Logic and Control System", GA91-9201-0002-00073 (3D-GD-A0008), Rev.4, June 2017.

[Ref-30] Hitachi-GE Nuclear Energy Ltd., "Topic Report on Dropped Loads Assessment of Nuclear Special Cranes", GA91-9201-0001-00205 (LE-GD-0249), Rev.1, March 2017.

[Ref-31] Hitachi-GE Nuclear Energy Ltd., "Standard Control Procedure for Identification and Registration of Assumptions, Limits and Conditions for Operation", GA91-0512-0010-00001(XD-GD-0042), Rev.2, March 2017

[Ref-32] Hitachi-GE Nuclear Energy Ltd., "UK ABWR Nuclear Safety and Environmental Design Principles (NSEDPs)"(XD-GD-0046), GA10-0511-0011-00001, Rev.1, July 2017

[Ref-33] Hitachi-GE Nuclear Energy Ltd., "Internal Flooding Evidence Report'' GA91-9201-0003-02122 (SE-GD-0612), Rev.1, June 2017.

[Ref-34] Hitachi-GE Nuclear Energy Ltd., "Internal Hazards Barrier Substantiation Report'' GA91-9201-0003-00426, BKE-GD-0019, Rev.5, July 2017.

[Ref-35] Hitachi-GE Nuclear Energy Ltd., "Topic Report on HP Turbine Casing Structural Integrity'' GA91-9201-0001-00278(CXJ-GD-1013), Rev.0, June 2017.

[Ref-36] Hitachi-GE Nuclear Energy, Ltd., "Detailed Analysis of Fire and Explosion Modelling and Barrier Response", GA91-9201-0003-01080, BKE-GD-0048, Rev.2, March 2017.

[Ref-37] Hitachi-GE Nuclear Energy, Ltd., "Diversity in Detection of Fault Sequences", GA91-9201-0003-00987, 3E-GD-A0186, Rev.0, October 2015.

[Ref-38] Hitachi-GE Nuclear Energy, Ltd., "Topic Report for Electrical Installation", GA91-9201-0001-00126, EE-GD-B008, Rev.2, April 2017.

[Ref-39] Hitachi-GE Nuclear Energy Ltd., "Equipment Design Environment Specification," GA11-1001-0004-00001, HPD-GD-H005, Rev.1, June 2017.

[Ref-40] Hitachi-GE Nuclear Energy Ltd., "Internal Blast Modelling Report", GA91-9201-0003-01420, SE-GD-0474, Rev.1, December 2016.

[Ref-41] Hitachi-GE Nuclear Energy Ltd., "General Design Process Approach for Mechanical Engineering SSCs", GA91-9201-0003-00854(SE-GD-0297), Rev.1, September 2016.

[Ref-42] Hitachi-GE Nuclear Energy Ltd., "Topic Report on HVAC penetrations on Class 1 Barriers", GA91-9201-0001-00186(SE-GD-0356), Rev.1, December 2016.

[Ref-43] International Electrotechnical Commission, "Electromagnetic compatibility (EMC) - Part 1: General - Section 1: Application and interpretation of fundamental definitions and terms", IEC TR 61000-1-1:Ed1.0, May 1992.

[Ref-44] Hitachi-GE Nuclear Energy Ltd., "Claim-Argument-Evidence Map of Internal Hazards Documents", GA91-9201-0003-02286(SE-GD-0648), Rev.0, August 2017.

Appendix A: Safety Functional Claims Table

Note: The formal approach to SFCs (Safety Functional Claims) described in the "GDA Safety Case Development Manual" (GA10-0511-0006-00001) is a systems engineering approach largely focusing on SSCs. Therefore the SFC approach will not be formally applied to Internal Hazard claims. However, the claims in section 7.3.1.5 are identified in the following Table (under "Claim ID") using the SFC notation to keep consistency with the other PCSR Chapters.
This table shows only claims but Claim – Argument – Evidence traceablity is shown in C-A-E map document [Ref-44].

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
1	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_SFC_5-7.1	Internal hazards do not prevent the delivery of the Fundamental Safety Functions.
2	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_SFC_5-7.2	The consequences of any internal hazard are limited to one division, except for areas covered by General Claim IH_SFC_5-7.3.
3	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_SFC_5-7.3	Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after an internal hazard, to fulfil the Fundamental Safety Functions.
4	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_F_SFC_5-7.1	Any internal flood event within the design basis will not prevent delivery of the Fundamental Safety Functions.
5	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_F_SFC_5-7.2	The Class 1 divisional barriers segregating neighbouring divisions will be such that the consequences of a design basis flooding event in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.
6	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_F_SFC_5-7.3	Where there are exceptions to physical segregation, sufficient A-1 or A-2 signals and equipment are available, during and after the internal flood, to fulfil the Fundamental Safety Functions.

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
7	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_F_SFC_5-7.3.1	Where flooding affects multiple Class 1 divisions, protection features such as non-divisional flood barriers or qualification of individual SSCs will be such that the consequences of a design basis flooding event in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.
8	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_D_SFC_5-7.1	Any dropped load event within the design basis will not prevent delivery of the Fundamental Safety Functions.
9	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_D_SFC_5-7.2	The Class 1 divisional barriers segregating neighbouring divisions will be such that the consequences of design basis dropped/collapsed load events in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.
10	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_CM_SFC_5-7.1	An Internal Missile event within the design basis will not prevent delivery of the Fundamental Safety Functions.
11		Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_CM_SFC_5-7.1.1	Rotating equipment is only operated with the designed casing in place.
12	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_CM_SFC_5-7.2	The Class 1 divisional barriers segregating neighbouring divisions will be such that the consequences of a design basis internal missile event in one division will not prevent SSCs in neighbouring divisions delivering their Fundamental Safety Functions.

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
13	5	Others	5-7	Functions to limit the effect of hazard	-	No claim	Normal Conditions	IH_E_SFC_5-7.1	Any design basis EMI/RFI event originating from the UK ABWR GDA site will not prevent delivery of any required Fundamental Safety Functions.
14	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_HM_SFC_5-7.1	Any Hazardous Material permitted on-site within the design basis will not prevent delivery of the Fundamental Safety Functions.
15	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_HM_SFC_5-7.1.1	Hazardous materials will be limited as far as reasonably practicable during the detailed design phase of the ABWR design. The GDA design does not assess all areas of the ABWR design and therefore cannot reduce the hazardous materials in areas not yet assessed.
16	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_HM_SFC_5-7.1.2	Where possible locating the hazardous materials outside the safety classified area.
17	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_HM_SFC_5-7.1.3	Designing systems which use or store hazardous materials to appropriate standards.
18	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_HM_SFC_5-7.1.4	Mitigating the consequences of hazardous materials release.

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
19	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_TA_SFC_5-7.1	Transport Accident events within the design basis will not prevent delivery of the Fundamental Safety Functions.
20	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_TA_SFC_5-7.1.1	A design basis transport accident occurring outside of a safety classified building will not prevent the delivery of the Fundamental Safety Functions.
21	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_TA_SFC_5-7.1.2	A design basis transport accident occurring within a safety classified building will not prevent the delivery of the Fundamental Safety Functions.
22	5	Others	5-7	Functions to limit the effect of hazard	-	No claim	Normal Conditions	IH PA SFC 5-7.1	Pipeline Accident events within the design basis will not prevent delivery of the Fundamental Safety Functions.
23	5	Others	5-7	Functions to limit the effect of hazard	-	No claim	Normal Conditions	IH PA SFC 5-7.1.1	For the purposes of GDA, a pipeline accident hazard may be analysed by considering the consequences of the pipeline failure itself.
24	5	Others	5-7	Functions to limit the effect of hazard	-	No claim	Normal Conditions	IH MH SFC 5-7.1	Methane Hazard events within the design basis will not prevent delivery of the Fundamental Safety Functions.

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
25	5	Others	5-7	Functions to limit the effect of hazard	-	No claim	Normal Conditions	IH MH SFC 5-7.1.1	The internal hazard of methane generation from the ground is considered to be site specific stage and cannot therefore be assessed during GDA.
26	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_FE_PCV_SFC_5-7.3	Any Design Basis Internal Fire or Explosion event originating within the PCV will not prevent delivery of the Fundamental Safety Functions.
27	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ F_PCV_SFC_5-7.3	Any Design Basis Internal Flood event originating within the PCV will not prevent delivery of the Fundamental Safety Functions.
28	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ PJ_PCV_SFC_ 5-7.3	Any Design Basis Internal Pipe Whip or Jet event originating within the PCV will not prevent delivery of the Fundamental Safety Functions.
29	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ D_PCV_SFC_ 5-7.3	Any Design Basis Dropped Load event originating within the PCV will not prevent delivery of the Fundamental Safety Functions.
30	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ CM_PCV_SFC_ 5-7.3	Any Design Basis Internal Missile event originating within the PCV will not prevent delivery of the Fundamental Safety Functions

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
31	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_B_PCV _SFC _5-7.3	Any Design Basis Blast event originating within the PCV will not prevent delivery of the Fundamental Safety Functions
32	5	Others	5-7	Functions to limit the effect of hazard	-	No claim	Normal Conditions	IH SFC EMI PCV 5-7.3	EMI within the PCV is now considered as part of the overall R/B EMI case
33	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ FE_MCR_SFC_ 5-7.3	Any Design Basis Internal Fire or Explosion event originating within the MCR will not prevent delivery of the Fundamental Safety Functions
34	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ F_MCR_SFC_ 5-7.3	Any Design Basis Internal Flood event originating within the MCR will not prevent delivery of the Fundamental Safety Functions
35	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ D_MCR_SFC_ 5-7.3	Any Design Basis Dropped Load event originating within the MCR will not prevent delivery of the Fundamental Safety Functions
36	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_ CM_MCR_SFC_ 5-7.3	Any Design Basis Internal Missile event originating within the MCR will not prevent delivery of the Fundamental Safety Functions

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
37	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_FE_MSTR_SFC_5-7.3	Any Design Basis Internal Fire or Explosion event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions
38	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_F_MSTR_SFC_5-7.3	Any Design Basis Internal Flood event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions
39	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_PJ_MSTR_SFC_5-7.3	Any Design Basis Internal Pipe Whip or Jet event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions
40	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_D_MSTR_SFC_5-7.3	Any Design Basis Dropped Load event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions
41	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_B_MSTR_SFC_5-7.3	Any Design Basis Blast event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions
42	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_CM_MSTR_SFC_5-7.3	Any Design Basis Internal Missile event originating within the MSTR will not prevent delivery of the Fundamental Safety Functions

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
43	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.1	A design basis turbine disintegration event will not result in the loss of Fundamental Safety Functions due to turbine missile impact.
44	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.2	The frequency of turbine missile generation is minimised through good practice in plant design and operation.
45	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.2.1	Turbine disintegration during normal operation risk is minimised through design, manufacture, inspection, testing and maintenance.
46	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	TBC	IH_TB_SFC_5-7.2.2	Runaway over speed failure risk is further minimised via the provision of a high reliability over speed protection system.
47	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.3	Design basis missiles resulting from turbine disintegration do not perforate the outer structures of safety classified buildings.
48	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.3.1	Missile ejection from the HP rotor and the generator is prevented due to retention by casing and/or stator.

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
49	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.3.2	All credible mechanisms by which missiles are generated from LP rotors are established. All credible missiles are classified and their characteristics are determined.
50	5	Others	5-7	Functions to limit the effect of hazard	17.6	Turbine Missile	Power Operation	IH_TB_SFC_5-7.3.3	Design Basis Low Trajectory normal over speed missiles have insufficient energy to perforate the outer structure of safety classified buildings.
51	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_IHC_SFC_5-7.1	Any combination of internal hazards within the design basis will not prevent the delivery of the Fundamental Safety Functions.
52	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_IHC_SFC_5-7.1.1	Any potential event which gives rise to a design basis internal hazard to result in the occurrence of additional, secondary hazards is minimised in the design by measures such as segregation, separation and qualification of equipment.
53	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_IHC_SFC_5-7.1.2	The simultaneous or successive occurrence of two or more design basis internal hazards with a single, underlying cause will not result in a more onerous consequences than if any of the hazards were to occur in isolation.
54	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_IHC_SFC_5-7.1.3	The simultaneous or successive occurrence of two or more design basis internal hazard events without any direct causal link is of sufficiently low probability that any such scenarios can be screened out on the basis of frequency.

	Top Claim for Mechanical System						Safety Functional Claim for the mechanical system and components (SFC)		
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule (Bounding Fault)				
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071)		State	Claim ID	Claim Contents
55	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_IHC_SFC_5-7.2	The divisional barriers segregating neighbouring divisions will be such that an event occurring in one division which gives rise to a primary internal hazard will not cause a secondary, consequential internal hazard to occur in a neighbouring division. Where there are exceptions to segregation, these will be assessed on a case by case basis.
56	5	Others	5-7	Functions to limit the effect of hazard	5.3	Long term LOOP + Hazard (loss of one Division)	Fault Conditions	IH_IHC_SFC_5-7.3	Where divisions are not segregated by physical barriers, and hazard protection is provided by separation or local protection, combined hazards will not damage sufficient safety measures in multiple divisions to prevent the delivery of the FSFs.

Appendix B: Safety Properties Claims Table

The relationship between the internal hazard assessment presented in this Chapter and the Safety Property Claims (SPCs) used elsewhere in the PCSR is described below:

- The Chapters of the PCSR that specify the SFCs also specify corresponding SPCs for each of SSCs required for safety.
- SPCs are numbered in accordance with the rules presented in the Safety Case Development Manual [Ref-24].
- None of these SPCs are explicitly listed in this Chapter, or in the relevant topic report listed in Appendix C (Document Map). Instead they are tabulated in Appendices of the Basis of Safety Cases.
- This Chapter does not introduce any new SPCs, over and above those presented in the PCSR SSC required for safety Chapters and in their supporting BSCs. Hence no lists of SPCs are required in the Appendices to this Chapter.

Appendix C: Document Map