Revision	Approved by	Number of Pages
000	[signature]	77
Approval Date	12/11/2018	

General Nuclear System

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	HPR/GDA/PCSR/0019

Title:

Pre-Construction Safety Report
Chapter 19
Internal Hazards

This document has been prepared on behalf of General Nuclear System Limited (GNS) with the support of China General Nuclear Power Corporation (CGN) and Électricité de France S.A. (EDF).

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

DISTRIBUTION LIST

Recipients	Cross Box
GNS Executive	☐
GNS all staff	☐
GNS and BRB all staff	☒
CGN	☒
EDF	☒
Regulators	☒
Public	☒

MODIFICATION RECORD

Revision	Section	Page	Modification
000	ALL	ALL	First Issue

TABLE OF CONTENTS

19.1 List of Abbreviations and Acronyms

ACI	American Concrete Institute
AFCEN	French Association for Design, Construction and In-Service Inspection Rules for Nuclear Steam Supply System Components
ALARP	As Low As Reasonably Practicable
ARE	Main Feedwater Flow Control System [MFFCS]
ASME	American Society of Mechanical Engineers
BDA	Emergency Diesel Generator Building A
BDB	Emergency Diesel Generator Building B
BDC	Emergency Diesel Generator Building C
BDU	SBO Diesel Generator Building for Train A
BDV	SBO Diesel Generator Building for Train B
BEJ	Extra Cooling System and Fire Fighting Water Supply System Building
BEX	Equipment Access Building
BFX	Fuel Building
BNX	Nuclear Auxiliary Building
BPX	Personnel Access Building
BRX	Reactor Building
BSA	Safeguard Building A
BSB	Safeguard Building B
BSC	Safeguard Building C
BSI	British Standards Institution
BTP	Branch Technical Position (US)
BWX	Radioactive Waste Treatment Building
CAE	Claims, Arguments, Evidence
CGN	China General Nuclear Power Corporation
COMAH	Control of Major Accident Hazards

DBC	Design Basis Condition
DCL	Main Control Room Air Conditioning System [MCRACS]
DEC	Design Extension Condition
EMI	Electromagnetic Interference
ETC	EPR Technical Code
GDA	Generic Design Assessment
HEAF	High-energy Arcing Fault
HIC	High Integrity Component
HSE	Health and Safety Executive
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
MCR	Main Control Room
MOFIS	Systematic Modelling Solution to Fire Safety Design of NPP
MSQA	Management of Safety and Quality Assurance
NRC	Nuclear Regulatory Commission (US)
NUREG	Nuclear Regulatory Commission technical report designation (US)
ONR	Office for Nuclear Regulation (UK)
PCSR	Pre-Construction Safety Report
PMC	Fuel Handling and Storage System [FHSS]
PSA	Probabilistic Safety Assessment
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant System [RCS]
RG	Regulatory Guidance (US)
RGP	Relevant Good Practice
RI	Regulatory Issue
RO	Regulatory Observation
RPV	Reactor Pressure Vessel

RQ	Regulatory Query
SAP	Safety Assessment Principle (UK)
SFP	Spent Fuel Pool
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide (UK)
UK HPR1000	UK version of the Hua-long Pressurised Reactor
VVP	Main Steam System [MSS]
WENRA	Western European Nuclear Regulators Association

System codes (XXX) and system abbreviations (YYY) are provided for completeness in the format (XXX [YYY]), e.g. Reactor Coolant System (RCP [RCS]).

19.2 Introduction

The main objective of Pre-Construction Safety Report (PCSR) Chapter 19 is to demonstrate that threats to nuclear safety from internal hazards are removed, minimised or tolerable for the UK version of the Hua-long Pressurised Reactor (UK HPR1000).

Internal hazards are those hazards to the facility or its structures, systems and components that originate within the site boundary and over which the dutyholder has control in some form, Reference [1].

Internal hazards have the potential to cause adverse conditions for Structures, Systems and Components (SSCs) necessary for fulfilling the following three fundamental safety functions given in Reference [2]:

a) Control of reactivity;

b) Removal of heat from the reactor and from the fuel store;

c) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

This sub-chapter presents the route map and the structure of Chapter 19, and interfaces with other chapters.

19.2.1 Chapter Route Map

This sub-chapter presents the claims, arguments and evidence (CAE) of Chapter 19, which are developed based on the Route Map shown in Chapter 1.

The ***Fundamental Objective*** of the UK HPR1000 is that: *The Generic UK HPR1000* *could be constructed, operated, and decommissioned in the UK on a site bounded by the generic site envelope in a way that is safe, secure and that protects people and the environment.*

To underpin this objective**,** five high level claims (Level 1 claims) and a number of Level 2 claims are developed and presented in Chapter 1. ***Claim 3, Claim 3.2, Claim 3.2.1 and Claim 3.2.2*** (from Chapter 1) are applicable to Chapter 19. The high level claims state that:

Claim 3: *The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defence to fulfil the fundamental safety functions, reducing the nuclear safety risks to a level that is as low as reasonably practicable.*

Claim 3.2: *A comprehensive fault and hazard analysis has been used to specify the requirements on the safety measures.*

To support ***Claim 3.2.1*** and ***Claim 3.2.2*** (from Chapter 1) derived from ***Claim 3.2***, Chapter 19 developed several sub-claims and a number of relevant arguments and associated evidence:

Claim 3.2.1: *All initiating events with the potential to lead to significant radiation exposure or release of radioactive material, including the effects of internal and external hazards have been identified.*

a) ***Sub-claim 1:*** *The individual internal hazards and hazard combinations that can potentially cause initiating faults and thus affect nuclear safety are sufficiently identified.*

   1) ***Argument 1.1:*** *All potential individual internal hazards are identified and screened through a comprehensive and reasonable process.*

   2) ***Argument 1.2:*** *All credible hazard combinations associated with the internal hazards are identified and screened through a comprehensive and reasonable process.*

Claim 3.2.2: *Design basis events have been appropriately assessed to specify requirements on safety functions and on safety measures and assess their effectiveness.*

b) ***Sub-claim 2:*** *Design basis internal hazards*[1] *are assessed to identify requirements on safety measures and assess their effectiveness.*

   For each internal hazard, the sub-claims, arguments and evidence are developed, including how the safety functions are ensured by provision of safety measures

[1] Design basis internal hazards refer to internal hazards that could be caused by credible internal hazard sources within the nuclear power plants and that could lead to unfavourable consequences.

and the effectiveness of these safety measures. At the current phase, the evidence has not been fully provided. The evidence will be completed in Generic Design Assessment (GDA) step 3 and step 4.

The nomenclature of the following sub-claims and arguments uses a convention that is hierarchical and retains the origin of the higher claims. For example, “Sub-claim_Fire_2.1” is a sub-claim made for internal fire which supports “Sub-claim 2”.

Internal Fire

1) ***Sub-claim_Fire_2.1:*** *The internal fire sources are sufficiently identified.*

   - ***Argument_Fire_2.1.1:*** *All of the combustible materials are identified, including the location and the fire loads.*

2) ***Sub-claim_Fire_2.2:*** *After undertaking the safety assessment, the safety measures to mitigate the consequences of internal fire are sufficiently identified and properly classified.*

   - ***Argument_Fire_2.2.1:*** *In segregation areas, safety measures are identified to ensure that the consequences of any internal fire are limited to one train of the systems delivering the safety functions through use of barriers.*

   - ***Argument_Fire_2.2.2:*** *Where there are exceptions to segregation, safety measures are identified to ensure that sufficient SSCs are available, during and after an internal fire, to deliver the safety functions.*

   - ***Argument_Fire_2.2.3:*** *The safety measures to mitigate the consequences of internal fire are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

3) ***Sub-claim_Fire_2.3:*** *The safety measures to mitigate the consequences of internal fire are sufficiently substantiated.*

   - ***Argument_Fire_2.3.1:*** *Divisional barriers between different safety fire compartments have a sufficient fire resistance rating.*

   - ***Argument_Fire_2.3.2:*** *Divisional barriers between different safety fire cells could effectively prevent the fire from spreading.*

   - ***Argument_Fire_2.3.3:*** *Functional fire resistant cases and cable wrappings could effectively protect SSCs important to safety in some areas where the multiple trains are in a given division.*

Internal Explosion

1) ***Sub-claim_Explosion_2.1:*** *The internal explosion sources are sufficiently*

identified.

2) ***Sub-claim_Explosion_2.2:*** *After undertaking the safety assessment, the safety measures to mitigate the consequences of internal explosion are sufficiently identified and properly classified.*

   - ***Argument_Explosion_2.2.1:*** *In segregation areas, safety measures are identified to ensure that the consequences of any internal explosion are limited to one train of the systems delivering the safety functions through use of barriers.*

   - ***Argument_Explosion_2.2.2:*** *Where there are exceptions to segregation, safety measures are identified to ensure that sufficient SSCs are available, during and after an internal explosion, to deliver the safety functions.*

   - ***Argument_Explosion_2.2.3:*** *For the explosion sources outside the buildings important to safety while within the site, safety measures are identified to ensure that the explosion does not jeopardise the buildings important to safety.*

   - ***Argument_Explosion_2.2.4:*** *The safety measures to mitigate the consequences of internal explosion are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

3) ***Sub-claim_Explosion_2.3:*** *The safety measures to mitigate the consequences of internal explosion are sufficiently substantiated.*

   - ***Argument_Explosion_2.3.1:*** *Divisional barriers can effectively withstand the overpressure from the explosion inside.*

   - ***Argument_Explosion_2.3.2:*** *Structures of the buildings important to safety could effectively resist the overpressure outside.*

Internal Flooding

1) ***Sub-claim_Flooding_2.1:*** *The internal flooding sources are sufficiently identified.*

2) ***Sub-claim_Flooding_2.2:*** *After undertaking the safety assessment, the safety measures to mitigate the consequences of internal flooding are identified and properly classified.*

   - ***Argument_Flooding_2.2.1:*** *In segregation areas, barriers are designed to ensure that the consequences of any internal flooding are limited to one train of the systems delivering the safety functions.*

   - ***Argument_Flooding_2.2.2:*** *Where there are exceptions to segregation, functional analysis is carried out to identify the safety measures to* *ensure sufficient SSCs are available, during and after an internal flooding, to deliver the safety functions.*

- ***Argument_Flooding_2.2.3:*** *The safety measures to mitigate the consequences of internal flooding are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

- ***Argument_Flooding_2.2.4:*** *Where required, SSCs important to safety are capable of delivering the safety functions in a submerged/ spray environment.*

3) ***Sub-claim_Flooding_2.3:*** *The safety measures for internal flooding are sufficiently substantiated.*

   - ***Argument_Flooding_2.3.1:*** *Barriers between different internal flooding zones can withstand the loading imposed by flooding associated with the maximum flooding level.*

   - ***Argument_Flooding_2.3.2:*** *If human actions are required, the required time to detect and diagnose and mitigate internal flooding is assessed and the achievability of human actions is demonstrated.*

High Energy Pipe Failures

1) ***Sub-claim_HEPF_2.1:*** *The high energy pipe failures sources are sufficiently identified.*

   - ***Argument_HEPF_2.1.1:*** *Gross failure is deterministically assumed to occur for all high energy pipes, except for pipes designed as high integrity component.*

2) ***Sub-claim_HEPF_2.2:*** *After undertaking the safety assessment, the safety measures to mitigate the consequences of high energy pipe failures are sufficiently identified and properly classified.*

   - ***Argument_HEPF_2.2.1:*** *In segregation areas, the consequences of any high energy pipe failures are limited to one train of the systems delivering the safety functions through use of barriers.*

   - ***Argument_HEPF_2.2.2:*** *Where there are exceptions to segregation, consequences of high energy pipe failures can be restricted through additional safety measures (e.g. shields, restraints, geometrical separation) so as to ensure the delivery of the safety functions.*

   - ***Argument_HEPF_2.2.3:*** *The safety measures to mitigate the consequences of high energy pipe failures are classified according to certain criteria in line with the methodology of safety categorisation and* *classification.*

- ***Argument_HEPF_2.2.4:*** *Where required, SSCs important to safety are capable to operate following a high energy pipe failure in the resulting environmental conditions.*

3) ***Sub-claim_HEPF_2.3:*** *The safety measures to mitigate the consequences of high energy pipe failures are sufficiently substantiated.*

   - ***Argument_HEPF_2.3.1:*** *Barriers have the capability of withstanding the loading imposed by high energy pipe failures.*

Dropped Loads

1) ***Sub-claim_Dropped_2.1:*** *The dropped loads sources are sufficiently identified.*

2) ***Sub-claim_Dropped_2.2:*** *After undertaking the safety assessment, the safety measures to mitigate the consequences of dropped loads are sufficiently identified and properly classified.*

   - ***Argument_Dropped_2.2.1:*** *In segregation areas, divisional barriers are used to ensure that the consequences of any dropped load are limited to one train of the systems delivering the safety functions.*

   - ***Argument_Dropped_2.2.2:*** *Where there are exceptions to segregation, functional analysis is carried out to identify the safety measures to ensure sufficient SSCs are available, during and after dropped loads, to deliver the safety functions.*

   - ***Argument_Dropped_2.2.3:*** *The safety measures to mitigate the consequences of dropped loads are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

3) ***Sub-claim_Dropped_2.3:*** *The safety measures to mitigate the consequences of dropped loads are sufficiently substantiated.*

   - ***Argument_Dropped_2.3.1:*** *The floors can withstand the impact of dropped loads and cannot fail in the event of a dropped load.*

   - ***Argument_Dropped_2.3.2:*** *Divisional barriers can withstand the impact of dropped loads.*

   - ***Argument_Dropped_2.3.3:*** *Validation of lifting procedure execution and lifting route planning can contribute to avoiding unacceptable consequences highlighted by the safety assessment.*

Internal Missiles

1) ***Sub-claim_Missiles_2.1:*** *The internal missile sources are sufficiently*

identified.

- ***Argument_Missiles_2.1.1:*** *Equipment is identified as potential internal missiles sources regardless of its classification except for equipment designed as high integrity component.*

- ***Argument_Missiles_2.1.2:*** *Although the probability of failure of an essential SSC due to turbine missiles is extremely low, turbine missile has been identified as potential internal missile source and assessed in both deterministic and probabilistic approaches.*

2) ***Sub-claim_Missiles_2.2****: After undertaking the safety assessment, the safety measures to mitigate the consequences of internal missiles are sufficiently identified and properly classified.*

- ***Argument_Missiles_2.2.1:*** *In segregation areas, safety measures are identified to ensure that the consequences of any internal missile are limited to one train of the systems delivering the safety functions through use of barriers.*

- ***Argument_Missiles_2.2.2:*** *Where there are exceptions to segregation, safety measures are identified to ensure that sufficient SSCs are available, during and after an internal missile, to deliver the safety functions.*

- ***Argument_Missiles_2.2.3:*** *The safety measures to mitigate the consequences of internal missiles are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

3) ***Sub-claim_Missiles_2.3:*** *The safety measures to mitigate the consequences of internal missiles are sufficiently substantiated.*

- ***Argument_Missiles_2.3.1:*** *Barriers between different divisions are substantiated to withstand the loading imposed by internal missiles.*

- ***Argument_Missiles_2.3.2:*** *Walls/ floors/ additional local partitions which are claimed to have the function of internal missile protection are also substantiated to withstand the loading imposed by internal missiles.*

Electromagnetic Interference (EMI)

1) ***Sub-claim_EMI_2.1****: The safety measures to mitigate the consequences of EMI are sufficiently identified.*

- ***Argument_EMI_2.1.1:*** *Isolation measures are adopted as they can have a significant effect on reducing the pervasiveness of the EMI hazard.*

- ***Argument_EMI_2.1.2:*** *Shielding measures are adopted as they can have a significant effect on reducing the pervasiveness of the EMI hazard.*

- ***Argument_EMI_2.1.3:*** *Electronic and Instrumentation and Control (I&C) equipment is designed and qualified to reduce the susceptibility to EMI effects.*

2) ***Sub-claim_EMI_2.2:*** *The safety measures to mitigate the consequences of EMI are sufficiently substantiated.*

Toxic and Corrosive Materials and Gases

1) ***Sub-claim_Toxic_2.1:*** *The toxic and corrosive materials and gases sources are sufficiently identified.*

2) ***Sub-claim_Toxic_2.2:*** *The release of toxic and corrosive materials and gases does not cause the loss of the safety functions.*

   - ***Argument_Toxic_2.2.1:*** *The MCR remains habitable in the event of a release of toxic and corrosive materials and gases.*

   - ***Argument_Toxic_2.2.2:*** *Sufficient systems are available, during the release of toxic and corrosive materials and gases, to deliver the safety functions.*

   - ***Argument_Toxic_2.2.3:*** *The safety measures to mitigate the consequences of Toxic and corrosive materials and gases release are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

Vehicular Transport Impact

1) ***Sub-claim_Vehicle_2.1:*** *The vehicular transport impact sources are sufficiently identified.*

   - ***Argument_Vehicle_2.1.1:*** *All the vehicles that can approach or enter the buildings important to safety are identified as vehicular transport impact sources.*

   - ***Argument_Vehicle_2.1.2:*** *The vehicular transport impact sources are divided into two types according to the impact location: inside or outside the buildings important to safety.*

2) ***Sub-claim_Vehicle_2.2:*** *The safety measures to mitigate the consequences of vehicular transport impact are sufficiently identified and properly classified.*

   - ***Argument_Vehicle_2.2.1:*** *Systems and components important to safety are protected from the vehicular transport impact outside the buildings.*

     - ***Argument_Vehicle_2.2.1.1:*** *The plant layout and transport route are well designed to avoid the consequence of vehicular transport impact outside the buildings.*

- ***Argument_Vehicle_2.2.1.2:*** *Structures of buildings important to safety have the capacity to withstand the load caused by vehicular transport impact outside the buildings.*

- ***Argument_Vehicle_2.2.2:*** *Systems and components important to safety are sufficiently segregated and protected from the consequences of vehicular transport impact inside the building.*

  - ***Argument_Vehicle_2.2.2.1:*** *Vehicle access to buildings important to safety is limited to specific areas.*

  - ***Argument_Vehicle_2.2.2.2:*** *Structures of buildings important to safety have the capacity to withstand the load caused by vehicular transport impact inside the building.*

- ***Argument_Vehicle_2.2.3:*** *The safety measures to mitigate the consequences of vehicular transport impact are classified according to certain criteria in line with the methodology of safety categorisation and classification.*

3) ***Sub-claim_Vehicle_2.3:*** *The safety measures to mitigate the consequences of vehicular transport impacts are sufficiently substantiated.*

   - *.**Argument_Vehicle_2.3.1:*** *Bounding case is used to qualify the ability of structures to withstand the load caused by vehicular transport impact outside the building.*

   - ***Argument_Vehicle_2.3.2:*** *Bounding case is used to qualify the ability of structures to withstand the load caused by vehicular transport impact inside the building.*

Hazard Combinations

1) ***Sub-claim_Combination_2.1:*** *After undertaking the safety assessment, the safety measures to mitigate the consequences of hazard combinations are sufficiently identified and properly classified.*

2) ***Sub-claim_Combination_2.2:*** *The safety measures to mitigate the consequences of hazard combinations are sufficiently substantiated.*

19.2.2 Chapter Structure

To better structure the safety case for the internal hazards area, Chapter 19 firstly gives the general principles, the assessment scope and the general approach in Sub-chapter 19.4. The contents described in Sub-chapter 19.4 are considered in the process of identification of types of internal hazards and in the safety assessment process. The CAE made on identification of internal hazards as well as credible hazard combinations are given in Sub-chapter 19.5. After identifying these hazards, Sub-chapter 19.6 presents the CAE on assessment of internal hazards. Sub-chapter 19.7 presents the CAE on assessment of hazard combinations. The combination of these claims demonstrates that all internal hazards as well as their combinations will not cause the loss of the delivery of safety functions. Sub-chapter 19.8 presents the results of the As Low As Reasonably Practicable (ALARP) assessment to ensure that the risk of internal hazards is reduced to be ALARP.

Chapter 19 of Internal Hazards is structured as follows:

a) Sub-chapter 19.1 lists the abbreviations and acronyms, which helps the understanding of the abbreviations and acronyms used in the Chapter 19;

b) Sub-chapter 19.2 provides general information about this chapter, including the route map, the chapter structure as well as interfaces with other chapters;

c) Sub-chapter 19.3 presents the applicable codes and standards of Chapter 19;

d) Sub-chapter 19.4 presents the general considerations of internal hazards, including the general principles and general safety assessment approach to be adopted for assessing internal hazards, and categorises the buildings types from the point of view of safety analysis;

e) Sub-chapter 19.5 presents identification of individual internal hazards as well as credible hazard combinations;

f) Sub-chapter 19.6 presents the assessment of individual internal hazards;

g) Sub-chapter 19.7 presents the assessment of hazard combinations;

h) Sub-chapter 19.8 presents the ALARP assessment;

i) Sub-chapter 19.9 presents the concluding remarks;

j) Sub-chapter 19.10 presents the references of this chapter.

19.2.3 Interfaces with Other Chapters

The sub-chapter presents interfaces between this chapter and other chapters which are listed in T-19.2-1.

T-19.2-1 Interfaces between Chapter 19 and Other Chapters

PCSR Chapter	Interface
Chapter 1 Introduction	Chapter 1 presents the Fundamental Objective, Level 1 Claims and Level 2 Claims which are partly supported by the claims, sub-claims and arguments presented in Sub-chapter 19.2.1.

PCSR Chapter	Interface
Chapter 2 General Plant Description	Chapter 19 presents the types of internal hazards and the requirements for protection against internal hazards which are considered in the design of the layout mentioned in Chapter 2.
Chapter 4 General Safety and Design Principles	Chapter 19 provides the methodology for protection against internal hazards with the consideration of relevant principles presented in Chapter 4.
Chapter 6 Reactor Coolant System	The design of the Reactor Coolant System (RCP [RCS]) described in Chapter 6 considers the internal hazards defined in Chapter 19. Chapter 6 provides the reactor coolant system design substantiation of applied hazard protection design principles presented in Chapter 19.
Chapter 7 Safety Systems	The design of the safety systems described in Chapter 7 considers the internal hazards defined in Chapter 19. Chapter 7 provides the safety systems design substantiation of applied hazard protection design principles presented in Chapter 19.
Chapter 8 Instrumentation and Control	The design of the I&C systems described in Chapter 8 considers the internal hazards defined in Chapter 19. Chapter 8 provides the I&C systems design substantiation of applied hazard protection design principles presented in Chapter 19.
Chapter 9 Electric Power	The design of the electrical power systems described in Chapter 9 considers the internal hazards defined in Chapter 19. Chapter 9 provides the electric power systems design substantiation of applied hazard protection design principles presented in Chapter 19.
Chapter 10 Nuclear Auxiliary Systems	The design of the auxiliary systems described in Chapter 10 considers the internal hazards defined in Chapter 19. Chapter 10 provides the auxiliary systems design substantiation of applied hazard protection design principles presented in Chapter 19.
Chapter 11 Steam and Power Conversion System	The design of steam and power conversion systems described in Chapter 11 considers the internal hazards

PCSR Chapter	Interface
	defined in Chapter 19. Chapter 11 provides the steam and power conversion systems design substantiation of applied hazard protection design principles presented in Chapter 19.
Chapter 12 Design Basis Condition	Chapter 12 presents the list of Design Basis Condition (DBC) which is identified from the postulated initiating events. Chapter 19 provides the supplement for postulated initiating events identification.
Chapter 14 Probabilistic Safety Assessment	Chapter 19 provides types of internal hazards considered in the UK HPR1000 and associated assessment results to support the internal hazards elements of the Probabilistic Safety Assessment (PSA). Chapter 14 evaluates the risk of internal hazards and provides risk insights to support the design of internal hazards.
Chapter 15 Human Factors	Chapter 19 provides human-related claims in internal hazards. Chapter 15 substantiates the claims on operator actions relating to internal hazards.
Chapter 16 Civil Works & Structures	Chapter19 defines internal hazards that lead to loads being placed on the civil structures. Chapter 16 presents the design substantiation of civil structures.
Chapter 17 Structural Integrity	Structural integrity demonstration mentioned in Chapter 17 considers types and assessment results of internal hazards presented in Chapter 19.
Chapter 18 External Hazards	Internal hazards potentially caused by external hazards are described in Chapter 18.
Chapter 20 MSQA and Safety Case Management	Chapter 20 sets out the organizational arrangements and Quality Assurance arrangements, which are implemented in Chapter 19.
Chapter 23 Radioactive Waste Management	The design of radioactive waste management systems described in Chapter 11 considers the internal hazards defined in Chapter 19.
Chapter 24 Decommissioning	Based on the list of internal hazard presented in Chapter 19, Chapter 24 has determined the internal hazards needed to be considered in decommissioning.
Chapter 25 Conventional Safety and Fire Safety	Chapter 19 identifies the internal hazard “Toxic and Corrosive Materials and Gases”. Specific personnel

PCSR Chapter	Interface
	safety protection against this hazard is described in Chapter 25. Chapter 25 and Chapter 19 have an interface in terms of internal fire protection design, especially in the design of fire areas, evacuation routes, and fire-fighting systems. Internal fire in Chapter 19 focuses on the nuclear safety while Chapter 25 is for life safety in the event of fire.
Chapter 28 Fuel Route and Storage	The design of the Fuel Handling and Storage System (PMC [FHSS]) described in Chapter 28 considers the internal hazards defined in Chapter 19. Chapter 19 identifies fuel handling devices as sources of dropped loads.
Chapter 33 ALARP Evaluation	Chapter 19 provides an ALARP assessment for internal hazards protection design by applying the ALARP methodology described in Chapter 33, which supports the overall ALARP demonstration.

19.3 Applicable Codes and Standards

In the UK HPR1000 design, the codes and standards applied in the design and assessment of protection against internal hazards are selected and determined mainly based on the selection principles and the selection process presented in Chapter 4. Details of the selection principles and selection process are presented in *General Principles for Application of Laws, Regulations, Codes and Standards,* Reference [3].

With considering necessary factors (e.g. design characteristics, UK regulatory expectations, requirements of guidance documents, Relevant Good Practice (RGP) and experience, etc.), the main selection principles are provided as follows, and the selected design codes and standards are:

a) The relevant good practice of international organizations (e.g. International Atomic Energy Agency (IAEA), Western European Nuclear Regulators Association (WENRA) etc.);

b) The experience used in other GDA projects;

c) The latest version (if an older version is selected, gap analysis is needed).

The selection process includes collection, screening, assessment, justification and analysis. A collection of international and national codes and standards that are international acknowledged and widely used in nuclear-industry, is implemented first. Then a screening process is carried out by applying the selection principles mentioned above. The codes and standards that are not commensurate with the selection principles are screened out. The assessment to these selected codes and standards considers several factors such as scope of application, degree of familiarity, application in practical engineering, relationship with the reference plant, etc. Based on the assessment result, the applicability, adequacy and sufficiency of codes and standards are identified and evaluated. The applicable codes and standards can be adopted, which is enough to support the design and justification.

The current identified applicable codes and standards for the design and the assessment of protection against internal hazards are listed as follows:

a) Common to all internal hazards

The following guidance documents issued by IAEA and WENRA are applicable to all internal hazards for protection design and assessment.

1) IAEA, Safety Requirements: Safety of Nuclear Power Plant: Design, No.SSR-2/1, Rev. 01, 2016, Reference [2];

2) WENRA, Safety Reference Levels for Existing Reactors, September 2014, Reference [4];

3) WENRA, Safety of New Nuclear Power Plant Design, March 2013, Reference [5].

b) Internal Fire

The *Safety Guide: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants,* Reference [6], is applicable in the design and the assessment of protection against internal fire and internal explosion. *ETC-F, 2010,* Reference [7], sets out the requirements on the internal fire protection with respect to the nuclear safety.

1) IAEA, Safety Guide: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.7, 2004, Reference [6];

2) AFCEN, EPR Technical Code for Fire Protection, ETC-F, 2010, Reference [7].

c) Internal Explosion

The Dangerous Substances and Explosive Atmospheres Regulations (DSEAR), Reference [8], is suitable for the design and the assessment of the protection against internal explosion.

1) IAEA, Safety Guide: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.7, 2004, Reference [6];

2) Health and Safety Executive, The Dangerous Substances and Explosive

Atmospheres Regulations, 2002 No.2776, 2002, Reference [8].

d) Internal Flooding

The *Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants*, Reference [9], is applicable in the design and the assessment of protection against internal hazards other than fires and explosions, including internal flooding, high energy pipe failures, dropped loads and internal missiles. The *Standard Review Plan* issued by Nuclear Regulatory Commission (NRC), Reference [10], is widely used in other GDA projects. Sub-chapter 3.4.1 of this guidance provides the requirements on internal flooding protection.

1) IAEA, Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.11, 2004, Reference [9];

2) NRC, Standard Review Plan, NUREG 0800, 2007, Reference [10].

e) High Energy Pipe Failures

The *Standard Review Plan* is widely used in other GDA projects. This guidance provides the principles on determination of pipe failure locations and failure mechanism (especially in Sub-chapter 3.6.2 of this guidance and Branch Technical Position (BTP) 3-3 and 3-4).

1) IAEA, Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.11, 2004, Reference [9];

2) NRC, Standard Review Plan, NUREG 0800, 2007, Reference [10].

f) Dropped Loads

The *Safety Guide: Design of Fuel Handling and Storage Systems for Nuclear Power Plants*, Reference [11], is applicable in the design and the assessment of protection against the drop of fuel and spent fuel cask. The guidance *Control of Heavy Loads at Nuclear Power Plants* (*NUREG 0612)*, Reference [12], is widely used in other GDA projects, which presents the assessment requirements, methods and protection requirements for dropped loads.

1) IAEA, Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.11, 2004, Reference [9];

2) IAEA, Safety Guide: Design of Fuel Handling and Storage Systems for Nuclear Power Plants, NS-G-1.4, 2003, Reference [11];

3) NRC, Control of Heavy Loads at Nuclear Power Plants, NUREG 0612, 1980,

Reference [12].

g) Internal Missiles

The guidance *Protection against Turbine Missiles* (*RG1.115)*, Reference [13], provides the design requirements for protection against turbine missiles. For example, it is required to consider an angle of 25 degrees to determine the influence scope from generated energetic missiles. In fact, an angle of more than 25 degrees is to be considered in the safety assessment of internal missiles.

1) IAEA, Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.11, 2004, Reference [9];

2) NRC, Protection against Turbine Missiles, RG1.115, 2012, Reference [13].

h) Toxic and Corrosive Materials and Gases

The Control of Major Accident Hazards (COMAH) Regulations are published in the UK. Compliance with the COMAH Regulations is required if the quantities of hazardous materials exceed the specified threshold in the regulations. The regulations require the operator to take necessary measures to limit the consequences to personnel and the environment.

1) Health and Safety Executive, The Control of Major Accident Hazards Regulations, 2015 No. 483, 2015, Reference [14].

i) Other Codes and Standards

The *Code Requirements for Nuclear Safety Related Concrete Structures and Commentary (ACI 349-13)* issued by American Concrete Institute (ACI) is used in civil design to perform the barrier substantiation in the internal hazards safety assessment. The complete codes and standards applicable to civil design are presented in Chapter 16.

1) American Concrete Institute, Code Requirements for Nuclear Safety Related Concrete Structures and Commentary, ACI 349-13, 2014, Reference [15];

19.4 General Considerations

This sub-chapter provides the general principles and requirements of hazards protection design, the assessment scope including the buildings to be considered, and the general safety assessment approach for internal hazards.

19.4.1 General Principles

The General Requirements of Protection Design against Internal and External Hazards, Reference [16], provides the general principles and the requirements of protection design against internal and external hazards. The main principles of protection design against internal hazards addressed in this document are as follows:

a) The defence in depth concept should be applied in the design of hazards protection. For example, the prevention is prior to safety measures;

b) Hazards should not result in the failure of any fundamental safety function of nuclear power plants;

c) Internal hazards should not cause DBC-3/4 or Design Extension Condition (DEC) events to the extent practicable. Even if this occurs, the delivery of the safety functions can be ensured;

d) Internal hazards shall not cause the failure of High Integrity Component (HIC);

e) Deterministic assessment uses conservative assumptions and single failure is assumed for assessment;

f) Priority should be given to passive barriers and the integrity of the barrier against individual and combined hazards should be substantiated. The acceptability of any partial loss of integrity should be assessed;

g) The habitability of the Main Control Room (MCR) should be ensured. The availability and the accessibility of the remote shutdown station should be ensured in case the MCR is unavailable;

h) The protection design measures should ensure that there is no cliff-edge effect.

19.4.2 Assessment Scope

According to *Scope for UK HPR1000 GDA Project*, Reference [17], Chapter 19 addresses internal hazards associated with the following key buildings important to safety and their adjacent buildings.

a) Reactor Building (BRX);

b) Safeguard Building A (BSA);

c) Safeguard Building B (BSB);

d) Safeguard Building C (BSC);

e) Fuel Building (BFX);

f) Emergency Diesel Generator Building A (BDA);

g) Emergency Diesel Generator Building B (BDB);

h) Emergency Diesel Generator Building C (BDC);

i) SBO Diesel Generator Building for Train A (BDU);

j) SBO Diesel Generator Building for Train B (BDV);

k) Radioactive Waste Treatment Building (BWX);

l) Nuclear Auxiliary Building (BNX);

m) Extra Cooling System and Fire Fighting Water Supply System Building (BEJ);

n) Personnel Access Building (BPX);

o) Equipment Access Building (BEX).

According to the layout feature, the above buildings are divided into two cases:

a) Segregation

The following buildings have been designed to incorporate hazard barriers to separate redundant trains of SSCs that deliver the safety functions into independent divisions:

1) BSA, BSB and BSC (except for the MCR in BSC, and the rooms/ areas in BSB simultaneously housing both train B and train C of the main steam lines and main feedwater lines and isolation valves);

2) BDA, BDB, BDC, BDU and BDV.

b) Exceptions to segregation

The following buildings or parts of those buildings are exceptions to segregation:

1) BRX;

2) BFX;

3) BWX;

4) BNX;

5) BEJ;

6) BPX;

7) BEX.

BRX and BFX are buildings containing redundant trains of systems and components important to safety that are required to deliver the safety functions. BNX and BWX are related to radioactive release, which contain Class 3 (F-SC3) equipment. BEJ contains redundant trains of F-SC3 systems and components. BPX and BEX are neighbouring buildings which may have the potential to impact the buildings containing systems and components important to safety.

19.4.3 General Safety Assessment Approach

F-19.4-1 is the general internal hazards safety assessment flowchart.

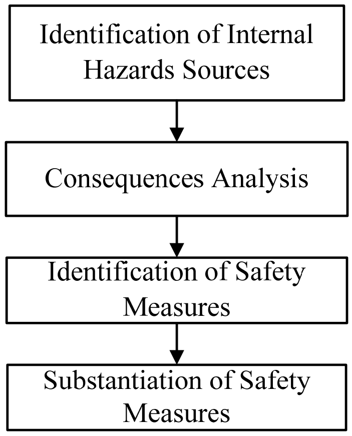
The internal hazards safety assessment process includes the following main steps:

a) Identification of internal hazards sources;

b) Consequences analysis;

c) Identification of safety measures;

d) Substantiation of safety measures.



F-19.4-1 Flowchart of Internal Hazards Safety Assessment

a) Identification of internal hazard sources

The first step is to identify the potential internal hazard sources. An internal hazard may occur where there are potential sources.

Therefore, the characteristics of internal hazard sources (e.g. location, quantity, property) will be identified first when carrying out the safety assessment of an internal hazard.

b) Consequences analysis

After identifying the sources, the consequences are analysed. For internal hazards, the consequences are analysed to verify that the delivery of safety functions is ensured. Target SSCs important to safety along with its safety class and divisions (i.e. trains) are identified and captured during the consequences analysis process. For most cases, the initial assumption for the consequences analysis is loss of all equipment within a hazard influenced scope.

c) Identification of safety measures

Based on the results of the consequences analysis, suitable and sufficient protection measures (including defence in depth measures) are identified for internal hazards.

d) Substantiation of safety measures

For substantiation of identified safety measures, the effects of internal hazards and credible hazard combinations on safety measures (e.g. barriers) are assessed to ensure that the safety measures do not fail under the internal hazard events. The characteristics of design basis internal hazards are quantified based on specified parameters if necessary. For example, a fire event is quantified in terms of the temperature-time profile on the hazard barriers, or a pipe whip event is quantified in terms of whip force. The loading being placed on safety measures for each internal hazard (or credible combinations) will be determined.

Production of a Hazard Schedule

The internal hazard sequence progress and associated safety measures are captured via production of a hazard schedule. The hazard schedule provides a summary of the assessments of all internal hazards, which gives the links between hazard identification, safety measures, safety classification, and where appropriate the postulated initiating events. The hazard schedule methodology is shown in Reference [18].

19.5 Identification of Internal Hazards

This sub-chapter presents the claims for identification of individual internal hazards as well as credible hazard combinations.

19.5.1 Individual Internal Hazard

The following argument supports Sub-claim 1 (see Sub-chapter 19.2.1):

Argument 1.1: All potential individual internal hazards are identified and screened through a comprehensive and reasonable process.

According to EHA.1 in *Safety Assessment Principles for Nuclear Facilities*, Reference [1], an effective process should be applied to identify and characterise all internal hazards that could affect the safety of the facility.

A comprehensive and systematic approach is used to identify credible internal hazards in the UK HPR1000. It takes into account all types of internal hazards referred to in the previous GDA projects. The types of internal hazards that are applicable to the UK HPR1000 are identified and screened in accordance with the following steps:

a) Identify the types of internal hazards according to the applicable codes, standards and guidance from UK organisations and international organisations, such as documents issued by IAEA, WENRA, etc.;

b) Refer to the previous GDA project experience feedback;

c) Determine which internal hazards can be screened out according to the potential consequences, and whether the failures induced by the hazard can be bounded by another hazard.

The detailed information about individual internal hazard identification and screening process is shown in Reference [19]. The internal hazards applicable to the UK HPR1000 are as follows:

a) Internal Fire;

b) Internal Explosion;

c) Internal Flooding;

d) High Energy Pipe Failures;

e) Dropped Loads;

f) Internal Missiles;

g) Electromagnetic Interference (EMI);

h) Toxic and Corrosive Materials and Gases;

i) Vehicular Transport Impact.

The assessment of individual internal hazards is detailed in Sub-chapter 19.6.

19.5.2 Hazard Combinations

The hazard combinations analysis should take into account simultaneous effects, common cause failures, defence in depth and consequential effects.

This sub-chapter describes the combination of internal hazards and the combination of internal hazards and design conditions. The combination of external hazard and internal hazard is described in Chapter 18.

The following argument supports Sub-claim 1 (see Sub-chapter 19.2.1):

Argument 1.2: All credible hazard combinations associated with the internal hazards are identified and screened through a comprehensive and reasonable process.

Hazard combinations associated with the internal hazards can be divided into the following categories:

a) Consequential hazards;

b) Correlated hazards;

c) Independent hazards;

d) Internal hazards and design condition.

All credible hazard combinations associated with the internal hazards are determined through a comprehensive and reasonable identification process, by applying an appropriate combination of engineering, deterministic and probabilistic method.

Consequential internal hazards identification

Consequential hazards are defined as the occurrence of a secondary hazard event that is directly caused by a primary hazard event. The identification and screening process is as follows:

a) Identifying the type of equipment whose failure could give rise to an internal hazard;

b) Identifying whether this type of equipment could be affected by the primary hazard or not.

For example, a pipe break could give rise to the internal flooding, and if this pipe is in the affected area of the dropped loads, the dropped loads (primary hazard) may cause the internal flooding (secondary hazard). Internal flooding is identified as a consequential hazard of dropped loads.

The preliminary list of consequential internal hazards is given in *The Identification and Screening Process of Internal and External Hazards*, Reference [19]. According to the system design and building layout of a nuclear power plant, comprehensive consideration will be made to determine which combinations of internal hazards are incredible or may be screened out.

Correlated internal hazards identification

Two or more internal hazards which occur as a result of a common cause are called correlated internal hazards. The identification and screening process is as follows:

a) Identifying the type of equipment whose failure could give rise to an internal hazard;

b) Identifying which two or more internal hazards have the same root cause.

For example, internal missiles and internal flooding are identified as correlated internal hazards because the failure of high pressurised vessel would give rise to both of them.

The preliminary list of correlated internal hazards is given in *The Identification and Screening Process of Internal and External Hazards*, Reference [19]. According to the system design and building layout of a nuclear power plant, comprehensive consideration will be made to determine which combinations of internal hazards are incredible or may be excluded.

Combination of independent internal hazards

Combinations of independent hazards are defined as the simultaneous occurrence of two or more hazard events which have no causal relationship among them. “Simultaneous” means that a second hazard occurs before the previous hazard has been completely mitigated. The identification and screening process is as follows:

a) Determining the frequency of each internal hazard;

b) Calculating the frequency of two or more independent hazards occurring simultaneously;

c) Comparing the frequency of two or more independent hazards occurring simultaneously with the cut-off frequency.

1×10^{-7} per annum (pa) is used as the cut-off frequency. The frequency of 1×10^{-5} pa is used to determine the design basis for the internal hazards. And the frequency of combination of independent internal hazards between 1×10^{-7} pa~1×10^{-5}pa is considered in the cliff edge analysis.

According to previous experience, the frequency of two or more internal hazards occurring simultaneously or within a short time period is extremely low. Further information is presented in Reference [19].

Combination of internal hazards and design condition

a) According to ETC-F 2010, Reference [7], fire is postulated to occur during normal operation (e.g. power operation or shutdown), or after reaching the controlled state of DBC-2, or after reaching the safe state of DBC-3/4, or in the post-accident long-term phase no earlier than two weeks after a DEC accident;

b) The internal hazards other than fire are only assumed to occur during normal operation (e.g. power operation or shutdown);

c) In principle, internal hazards should not result in DBC-3/4 or DEC; however, in practice, there may be some exceptions that should be considered in the design. In these cases, they should be analysed and assessed in detail to ensure their consequences are acceptable;

d) Internal hazards could potentially result from DBC-3/4 or DEC.

19.6 Assessment of Individual Internal Hazards

For each individual internal hazard, this sub-chapter presents claims, arguments and evidence on assessment of internal hazards by a process of identification of sources, safety assessment, identification of safety measures, and substantiation of safety measures. In addition, the defence in depth measures which are not claimed but also essential in protection design against these internal hazards are presented.

19.6.1 Internal Fire

19.6.1.1 Internal Fire Introduction

Internal fire is one of the main internal hazards which can threaten nuclear safety. The combustible materials in each room are defined as fire sources.

19.6.1.2 Internal Fire Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence regarding the internal fire hazard.

Sub-claim_Fire_2.1: The internal fire sources are sufficiently identified.

All the combustible systems and components in the UK HPR1000 are identified as internal fire sources. As such, the materials used in the UK HPR1000 are preferentially non-combustible. For instance, walls, ceilings and floors which are made of cement, bricks and reinforced concrete are non-combustible. And all of the insulation materials of electric cables are fire-retardant and are manufactured based on relevant UK standards (e.g. Reference [20]).

Argument_Fire_2.1.1: All of the combustible materials are identified, including the location and the fire loads.

There are a number of potential fire sources in the UK HPR1000 design, including:

a) Cables and electrical equipment;

b) Oil (e.g. lubrication oil);

c) Activated carbon in filter equipment;

d) Temporary combustible materials.

A collection and assessment work for the fire loads data in the buildings important to safety are carried out for the fire zoning design. The fire loads in field areas of the plant which are located away from buildings important to safety could be assessed simply (based on the distance, fire loads and fire resistance of the target buildings boundaries, etc.).

Sub-claim_Fire_2.2: After undertaking the safety assessment, the safety measures to mitigate the consequences of internal fire are sufficiently identified and properly classified.

With regards to internal hazards, there are two categories of areas: the first one is segregation areas and the second one is exception to segregation areas. Safety Fire Compartment (SFS) and Safety Fire Cell (ZFS) presented below indicate how the internal fire assessment is addressed within these two categories of areas.

SFS/ ZFS is designed to protect redundant safety divisions from common mode failure. SFS is created for the segregation area, while ZFS is created for the area where an entire segregation is not possible.

According to the requirements of Reference [7], the types of fire areas, related to safety, used in the UK HPR1000 are summarised in T-19.6-1.

T-19.6-1 Fire Areas Related to Safety

Codes	Description
SFS	The safety fire compartment
ZFS	The safety fire cell

According to the requirements of Reference [7]:

a) Fire area is a limited area to prevent the propagation of the fire, including fire compartment and fire cell;

b) A fire compartment is an area consisting of one or more rooms, bounded by partitions whose fire resistance guarantees that a fire occurring inside cannot extend to the outside or that one occurring on the outside cannot spread to the inside for a given period of time. All the partitions of a fire compartment shall be fire-resistant;

c) A fire cell is a fire area, bounded by partitions or boundaries which provide a guarantee that a fire occurring on the inside cannot extend to the outside or that one occurring on the outside cannot spread to the inside for a given period of time.

Argument_Fire_2.2.1: In segregation areas, safety measures are identified to ensure that the consequences of any internal fire are limited to one train of the systems delivering the safety functions through use of barriers.

For the segregation buildings, the systems and components important to safety are arranged in different divisions, and the fire compartments are used to limit the propagation of fire between different divisions by barriers. The barriers provide robust segregation as the boundaries (walls, pillars, ceiling, floor, doors, penetrations, etc.) between different fire areas have a fire resistance rating of 120 min.

Heating, Ventilation and Air Conditioning (HVAC) ducts are equipped with fire dampers. Service penetrations have the appropriate fire resistant seals. The number of such penetrations through the barriers should be minimised.

Argument_Fire_2.2.2: Where there are exceptions to segregation, safety measures are identified to ensure that sufficient SSCs are available, during and after an internal fire, to deliver the safety functions.

The fire cells are used to limit the spreading of fire in exception to segregation areas. The assessment for boundaries between different fire cells will be based on the approach provided in *Fire Analysis Methodology Report*, Reference [21]. As mentioned above, ZFS is created for the areas where entire segregation is not possible, so a 120 min fire resistance rating will also apply to the physical barriers of the ZFS, while for the opening (virtual boundary), the assessment should be conducted to demonstrate that a conservative fire scenario based on the fire loads could not spread to another fire cell through the opening.

In addition, it is necessary to carry out the common mode analysis in fire cells to ensure that the fire cannot affect the delivery of the safety functions, and the detailed analysis method can be found in Reference [21].

Argument_Fire_2.2.3: The safety measures to mitigate the consequences of internal fire are classified according to certain criteria in line with the methodology of safety categorisation and classification.

The barriers of fire areas provided to limit the effects of internal fire are classified on the basis of the consequences of internal fire.

The safety measures are classified according to certain criteria in line with the *Methodology of Safety Categorisation and Classification*, Reference [22]. According to Reference [22], functions provided to limit the effects of internal hazards within the design basis are categorised on the basis of the consequences of failure. For example, if the effects of an internal fire will cause the loss of a required Category 1 (FC1) safety function, the safety measures necessary to protect against internal fire are needed to be classified as Class 1 (F-SC1).

Sub-claim_Fire_2.3: The safety measures to mitigate the consequences of internal fire are sufficiently substantiated.

Argument_Fire_2.3.1: Divisional barriers between different safety fire compartments have a sufficient fire resistance rating.

The fire resistance duration test for barriers is presented in Sub-chapter 16.8. The fire resistance curve used for the test is given in *BS476 Part 20:1987*, Reference [23].

Argument_Fire_2.3.2: Divisional barriers between different safety fire cells could effectively prevent the fire from spreading.

The software *Systematic Modelling Solution to Fire Safety Design of NPP* (MOFIS) is used to assess the performance of the barriers of a fire cell. It will demonstrate that a fire in one fire cell cannot spread to the other fire cell nearby, if the consequences cannot be justified as acceptable, modification must be taken until the consequence is acceptable. Information on the assessment methodology is given in Reference [21].

Argument_Fire_2.3.3: Functional fire resistant cases and cable wrappings could effectively protect SSCs important to safety in some areas where the multiple trains are in a given division.

The purpose of fire common mode analysis is to determine whether a fire in a fire area could affect the delivery of the safety functions. If the analysis shows that the consequence of a fire is unacceptable, additional protection measures (fire resistant cases and cable wrappings) will be added or the layout design will be modified.

In this regard, the fire resistant cases and cable wrappings are similar to the barriers from an internal fire point of view, so the fire resistance rating should also be 120 min. The requirement for these measures is that the function of the cables or equipment covered by wrappings and cases should be ensured during a 120 min fire.

19.6.1.3 Defence in Depth Measures

In addition to the safety measures above, other defence in depth measures are incorporated in the design.

a) The following fire areas in T-19.6-2 are claimed to be defence in depth measures for fire protection:

T-19.6-2 Fire Areas Related to ‘Defence in Depth’

Codes	**Description**
SFA	The access compartment
SFI	The intervention fire compartment
ZFI	The unavailability limitation fire cell

1) The access compartment (SFA) is to enable the personnel to evacuate in full safety in the event of fire and to provide access to the fire-fighting teams. It is important to note that all of the access compartments are fully surrounded by a fire resistant boundary and provided with positive pressurisation. These areas shall not contain items important to safety and strictly minimise fire loads. Because the SFA is a safe and convenient route for fire fighter access, it could be considered as part of Defence in Depth measures;

2) The intervention fire compartment (SFI) or the unavailability limitation fire cell (ZFI) is created on the basis of the fire load inventory to limit the combustible materials with high fire loads to one area and to facilitate the intervention of fire fighters. The rooms with a risk of generalised fire (PFG) or a risk of localised fire (PFL) shall be partitioned as SFI/ ZFI. The detailed description for PFG/ PFL is given in Reference [21]. For other situations not complying with the PFG/PFL criteria, the judgement is based on engineering experience;

b) When there is a fire in the plant, mitigation measures should be taken immediately. To make sure the fire can be detected and extinguished as soon as possible, three fire protection systems are incorporated in the design:

1) Fire alarm systems;
2) Fire-fighting systems;
3) Smoke control systems.

Fire alarm systems

These systems are set for detecting fire at the early stage, and are generally incorporated in all buildings.

The fire alarm system can continuously monitor the plant through fire detectors that are placed in various locations. The system can quickly detect fire, automatically alarm, provide the exact location of fire area and monitor the development of a fire. The fire alarm system can initiate automatic actions when necessary. The alarm could aid operators in identifying the location of internal fire, and the period of time for operators to respond the events could be reduced.

Fire alarm control units are provided with a digital control system with all fire information necessary for the operation of fire protection system. The signal is confirmed by doubled detection. Further information about the fire alarm systems is given in Sub-chapter 10.7.3.

Fire-fighting systems

In UK HPR1000 design, the fire-fighting systems have been designed for specific high fire load areas to extinguish the fire when it occurs. The appropriate extinguishing agents have been selected according to the types of the combustible materials.

The fire-fighting systems are composed of two redundant fire-fighting water tanks of demineralised water and three fire fighting pumps each supplying 100% of the requirement for the most adverse point in the nuclear island. Note: two pumps are necessary for the most adverse requirement of the site which is located outside the nuclear island.

Fire-fighting systems include several sub-systems, and they serve different buildings or areas in the plant. Further information about the fire-fighting systems is given in Sub-chapter 10.7.4.

Smoke control system

Smoke control system has been set in the UK HPR1000 design to:

- Protect the SFAs from smoke (pressurised sub-system);
- Exhaust the smoke within the fire area.

Further information about the smoke control systems is presented in Sub-chapter 10.7.5.

19.6.1.4 Cliff Edge Effects

For fire, the cliff edge effects can be eliminated through the following strategy:

a) The ignition of any combustible material within the nuclear facility is considered;

b) The fire analysis is performed based on conservative assumptions such as the assumption that all the equipment is lost within the fire area;

c) Fire area verification can ensure that the fire boundary resistance rating of fire areas has sufficient margin, and fire common mode analysis can confirm that a fire will not lead to an unacceptable consequence;

d) In order to reduce the potential risk, additional protection measures are adopted according to the fire analysis results.

19.6.2 Internal Explosion

19.6.2.1 Internal Explosion Introduction

Internal explosion is an explosion which could occur within the site of the nuclear power plant. For example, an explosion may occur when explosive material leaks into the environment or high voltage electrical equipment fails etc. Explosions inside the plant can potentially damage SSCs important to safety.

Internal explosion is postulated to occur during normal operation (e.g. power operation or shutdown).

19.6.2.2 Internal Explosion Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence made regarding the internal explosion hazard.

Sub-Claim_Explosion_2.1: The internal explosion sources are sufficiently identified.

There are a number of potential explosion sources in the UK HPR1000 design:

a) Hydrogen (e.g. battery room);

b) Oil mist;

c) High-energy Arcing Fault (HEAF);

d) Blast wave from high pressure tanks or pipes.

The sources of explosion have been suppressed by the following items:

a) The use of removable devices on pipes containing explosive materials has been minimised or replaced by welded devices;

b) The use of explosive gases or pressurised tanks in buildings important to safety has been strictly limited;

c) Appropriate types of electrical equipment have been chosen to avoid HEAF;

d) The use of explosive or inflammable material has been specified taking explosion prevention into consideration.

The Dangerous Substances and Explosive Atmosphere Regulations, Reference [8], contains the schedule of hazardous substances. Sources of internal explosion are identified according to the Reference [8].

In general, the explosion sources in the UK HPR1000 are explosive gas release or production, HEAF, blast wave from high pressure vessels or pipes or oil mist diffusion. All of the locations with the explosion risk in the nuclear power plant site have been identified.

Sub-Claim_Explosion_2.2: After undertaking the safety assessment, the safety measures to mitigate the consequences of internal explosion are sufficiently identified and properly classified.

Based on the location of the explosion sources, the argument for explosion is divided into four parts:

Argument_Explosion_2.2.1: In segregation areas, safety measures are identified to ensure that the consequences of any internal explosion are limited to one train of the systems delivering safety functions through use of barriers.

For explosions in buildings which are important to safety, the aim is that an explosion should not jeopardise more than one train of the systems delivering the safety functions.

The systems and components important to safety in the segregation buildings are arranged in different divisions, and the barriers provide robust segregation against explosion between different divisions.

Argument_Explosion_2.2.2: Where there are exceptions to segregation, safety measures are identified to ensure that sufficient SSCs are available, during and after an internal explosion, to deliver the safety functions.

For the buildings or areas that are exceptions to segregation, it is difficult to limit the explosions to one division, so the functional analysis[2] is necessary to determine whether the explosion consequences are acceptable or not.

The internal explosion safety assessment methodology for areas considered as exceptions to segregation includes the following main steps:

[2] The functional analysis will be performed to confirm that adequate SSCs remain available to deliver the safety functions when a hazard affects more than one train in a given division.

a) Assessing the scenario of explosion, calculate the overpressure;

b) Assessing the affected rooms or area by a conservative and comprehensive consideration about the structure/opening/boundary for the areas and the overpressure;

c) Identifying the systems and components important to safety in the affected rooms or areas, and assuming that the systems and components in affected rooms or areas are lost;

d) Carrying out a functional analysis for the affected rooms or areas.

If the consequences of the explosion are unacceptable, the design should be modified. The detailed assessment method can be found in Reference [24].

Argument_Explosion_2.2.3: For the explosion sources outside the buildings important to safety while within the site, safety measures are identified to ensure that the explosion does not jeopardise the buildings important to safety.

There are explosion sources located in the field area or buildings without systems and components important to safety. The method to mitigate the consequences of these potential explosions is to ensure that the safe distance between explosion source and target (buildings important to safety) is sufficient.

Sufficient distance could attenuate the overpressure of the wave. When the overpressure wave finally reaches the position of the target building, it cannot affect the systems and components important to safety because the structure of the target buildings could prevent it from entering. This is similar to external explosion. The detailed information is provided in Reference [25].

Argument_Explosion_2.2.4: The safety measures to mitigate the consequences of internal explosion are classified according to certain criteria in line with the methodology of safety categorisation and classification.

Safety measures provided to limit the effects of internal hazards within the design basis are principally barriers.

The safety measures are classified according to certain criteria in line with the methodology of safety categorisation and classification, Reference [22]. According to Reference [22], functions provided to limit the effects of internal hazards within the design basis are categorised on the basis of the consequences of failure. For example, if the effects of an internal explosion will cause the loss of a required FC1 safety function, the safety measures necessary to protect against internal explosion are to be classified as F-SC1.

Sub-Claim_Explosion_2.3: The safety measures to mitigate the consequences of internal explosion are sufficiently substantiated.

The explosion sources are identified, and then the detection and ventilation measures which could prevent the accumulation of explosive gas are substantiated.

Argument_Explosion_2.3.1: Divisional barriers can effectively withstand the overpressure from the explosion inside.

Different types of explosions are analysed and the consequences of these explosions are assessed, and then a pressure-bearing assessment is conducted for the barriers against overpressure.

Argument_Explosion_2.3.2: Structures of the buildings important to safety could effectively resist the overpressure outside.

The building layout design considers the consequences of the overpressure calculation. TNT (2, 4, 6-Trinitrotolueneequivalence) is used to calculate the consequences of the explosion. The boundaries of the buildings important to safety are designed to withstand 10kPa overpressure, so the distance for pressure wave attenuation has been considered.

19.6.2.3 Defence in Depth Measures

For internal explosion, the following defence in depth measures are also incorporated in the design:

a) Grounding devices are installed in the areas with explosion risk to prevent the formation of electrical sparks;

b) Periodic testing of equipment is conducted;

c) The concentration of an explosive material required to activate the alarm is designed with sufficient safety margin based on the requirement from Reference [8].

19.6.2.4 Cliff Edge Effects

For internal explosion, the cliff edge effects can be eliminated through the following strategy:

a) It is important to consider the temporary storage of explosion materials, the change of storage quantity could impact the safety distance, the explosion risk, etc., enough margin should be considered in the protection design;

b) In order to reduce the potential risk, additional protection measures are adopted according to the explosion analysis, for example, if the concentration of an explosive material in the room approaches its Lower Explosion Limit (LEL), the additional leakage control is to be taken to reduce the risk of explosion;

c) The internal explosion analysis is performed based on conservative assumptions such as the application of the random failure principle to the isolation valves.

19.6.3 Internal Flooding

19.6.3.1 Internal Flooding Introduction

The internal flooding hazard is identified as one of the major internal hazards in nuclear power plants. Internal flooding can occur due to failure of pipework or tanks containing liquid. A design basis internal flooding hazard is conservatively postulated as gross failure (i.e. double ended guillotine break) of pipework or tanks occurring randomly from fluid containing systems during normal operation (e.g. power operation or shutdown). It can simultaneously disable multiple SSCs that are not designed against submergence or spray effect.

The internal flooding safety assessment considers the effects of submergence, spray and steam release. Condensed steam is also considered as a flooding source in the internal flooding safety assessment. The dynamic effects (i.e. pipe whip and jet impingement) due to high energy pipe failures are considered in Sub-chapter 19.6.4. Other effects (e.g. increase in humidity, radiation and temperature) resulting from a liquid release are considered in the qualification process for equipment in accordance with their safety significance.

19.6.3.2 Internal Flooding Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence regarding the internal flooding hazard.

Sub-claim_Flooding_2.1: The internal flooding sources are sufficiently identified.

All systems and components containing liquid (i.e. pipes, tanks/ vessels) in the UK HPR1000 are identified as potential internal flooding sources, except those designed as HIC which are justified in Chapter 17. All sources which could contribute to the total flooding volume, including sources that have no reliable isolation measures or that have inexhaustible supplies, are identified via a systematic identification process.

Sources outside the buildings but within the site boundary are also identified and analysed if they could enter the buildings and increase the total flooding volume.

Sub-claim_Flooding_2.2: After undertaking the safety assessment, the safety measures to mitigate the consequences of internal flooding are identified and properly classified.

For buildings housing equipment important to safety, safety measures are identified to protect against internal flooding. The principal safety measures to protect SSCs from the effects of internal flooding are barriers. The internal flooding zoning design is incorporated in the UK HPR1000 design, which is detailed in the *Internal Flooding Analysis Methodology Report*, Reference [26]. There are three types of internal flooding zones:

a) Common Mode Prevention Internal Flooding Zone

A common mode prevention internal flooding zone is defined in areas where there are segregated divisions. If such a zone is flooded and its safety function is lost, its redundant trains are still available. {

}

b) Forbidden Internal Flooding Zone

This type of internal flooding zone is created to protect safety functions when a complete physical segregation is not possible or to protect rooms/ areas with specific requirements { }. The boundaries of forbidden internal flooding zones can withstand the loading associated with the maximum flooding level. {

}

c) Non-safety Internal Flooding Zone

This type of internal flooding zone is created for the areas that do not belong to the above two types of internal flooding zones. { }The role of a non-safety internal flooding zone is to prevent the flooding in this zone from spreading to other types of internal flooding zones. {

}

Argument_Flooding_2.2.1: In segregation areas, barriers are designed to ensure that the consequences of any internal flooding are limited to one train of the systems delivering the safety functions.

In segregation areas, the common mode prevention internal flooding zones are incorporated into UK HPR1000 plant design. The barriers of this type of internal flooding zone are designed to meet watertight requirements and to limit the propagation of internal flooding from one division to another. The loss of one common mode internal flooding zone is considered to be acceptable and the barriers between different divisions are substantiated. The barrier substantiation is presented in Chapter 16.

Within a common mode internal flooding zone, a range of discharge routes (e.g. ordinary door gaps, unsealed penetrations/ openings, gratings, stairwells and elevators) are provided to allow the flooding to propagate both horizontally throughout the floor where the flooding is initiated and vertically to lower floors. The spread paths inside a common mode internal flooding zone will be presented in the detailed assessment report.

Argument_Flooding_2.2.2: Where there are exceptions to segregation, functional analysis is carried out to identify the safety measures to ensure sufficient SSCs are available, during and after an internal flooding, to deliver the safety functions.

In areas where exceptions to segregation exist, it is not reasonably practicable to segregate redundant equipment. Forbidden internal flooding zones are incorporated into the UK HPR1000.

For the purposes of internal flooding assessment, functional analysis is carried out to identify the safety measures to ensure that the consequences of internal flooding in these areas are acceptable and the delivery of safety functions is ensured.

The main exception to segregation areas in the design of the UK HPR1000 are in the Reactor Building, the MCR and the Main Steam System (VVP [MSS])/ Main Feedwater Flow Control System (ARE [MFFCS]) pipes and valves rooms. These areas have different design features:

a) The Reactor Building

The Reactor Building has double-walled (internal and external) containment. There are two “Forbidden Internal Flooding Zones” set in the Reactor Building: the internal containment and the annulus. The annulus is the area between the external containment and the internal containment. In the annulus, the principal flooding source is the fire-fighting systems, and there are only some pipelines, pipework penetrations and cables in the annulus. The flooding effects on these components do not affect the delivery of safety functions.

Within the internal containment, if flooding is initiated above 1.20m (the ground level of reactor building), liquid flows through structural openings on the floors to the lower level (i.e. basement) which contains a large storage volume. In addition, there are some partial barriers which separate different trains of safety systems at a distance. The maximum flooding levels in these rooms are determined and it is assessed if redundant SSCs important to safety are damaged.

b) The MCR

The MCR contains different trains of systems for its unique functions. So the MCR is divided as a forbidden internal flooding zone. There is no flooding source located in the MCR. Other flooding sources outside the MCR are prevented from propagating into this area through the layout design.

c) Other exception to segregation areas

There are also other exception to segregation areas housing redundant safety trains, for example, the VVP [MSS]/ ARE [MFFCS] pipes and valves rooms. Where this is the case, the maximum flooding levels in these rooms/ areas are calculated to assess whether redundant SSCs important to safety are damaged and whether the delivery of safety functions is impeded.

For exception to segregation areas, functional analysis is carried out to assess if redundant SSCs important to safety are damaged, whether these functions are required in this case and whether there are other means to deliver the safety functions. If the functions are necessary and there is no other means to deliver the same function, the consequences of internal flooding are considered to be unacceptable. And reliable, appropriately classified protection and mitigation measures are to be considered.

Argument_Flooding_2.2.3: The safety measures to mitigate the consequences of internal flooding are classified according to certain criteria in line with the methodology of safety categorisation and classification.

Barriers provided to limit the effects of internal flooding within the design basis are classified according to certain criteria in line with the *Methodology of Safety Categorisation and Classification*, Reference [22].

In addition, if detection and isolation measures are credited in the safety case, they are properly classified. In the UK HPR1000 design, the detection devices (such as pressure sensors and sump level sensors) provide early indication of an internal flooding hazard and alert the operators in the MCR. These detection devices are designed to meet corresponding safety classifications. The isolation measures (e.g. close an isolation valve, stop an operating pump, etc.) are provided to ensure that sources of flooding can be isolated and to prevent increases in flooding levels and subsequent damage to SSCs important to safety. The single failure criterion is applied to active components for mitigation of internal flooding effects.

According to Reference [22], functions provided to limit the effects of internal and hazards within the design basis are categorised on the basis of the consequences of failure. For example, if the effects of internal flooding cause the loss of a required FC1 safety function, the safety measures necessary to mitigate the flooding effects are to be F-SC1.

Argument_Flooding_2.2.4: Where required, SSCs important to safety are capable of delivering the safety functions in a submerged/ spray environment.

In the design of the UK HPR1000, equipment that is qualified to be operable under a submerged/ spray environment is assumed not to fail in the event of flooding. The equipment required to be qualified is identified after the safety assessment. In the event submergence/ spray effects cause the loss of SSCs important to safety within the affected areas, further assessment is performed. If redundant equipment important to safety is damaged, other mitigation measures that can be taken (e.g. isolation or elevation of equipment) are assessed. If these measures are not reasonably practicable, equipment important to safety is needed to be qualified to a suitable equipment specification to ensure their operability in a submerged/ spray environment.

Equipment qualification is detailed in the equipment technical specification and equipment qualification test reports consisting of equipment data and equipment qualification methods and results.

Sub-claim_Flooding_2.3: The safety measures for internal flooding are sufficiently substantiated.

Argument_Flooding_2.3.1: Barriers between different internal flooding zones can withstand the loading imposed by flooding associated with the maximum flooding level.

Barriers between different internal flooding zones are designed to meet watertight requirements. The barriers include walls, floors, penetrations, doors, etc.

The maximum flooding levels are calculated based on the maximum flooding volume in the principal areas of UK HPR1000. The building structures and penetrations are designed to remain intact following the resulting loads. Penetrations in the flooding resistant barriers are sealed to eliminate spread paths to adjacent internal flooding zones.

Argument_Flooding_2.3.2: If human actions are required, the required time to detect and diagnose and mitigate internal flooding is assessed and the achievability of human actions is demonstrated.

Where required, isolation by human actions, either in the MCR or by local, is considered in the internal flooding safety case. The required time to detect and diagnose and mitigate internal flooding is assessed and the achievability of human actions is demonstrated according to the methodology and requirements given in the Human Factors area (Chapter 15). According to Reference [22], human actions that are required to perform or to support a safety function are classified based on the significance of the safety function of SSCs.

The achievability of human actions in the MCR is demonstrated in an operator non-intervention time of 30min. Where local human actions are required, the required time to detect and diagnose and mitigate internal flooding is assessed. If human response time following the alarm is assessed higher than the required time (e.g. 1h), design provisions are to be implemented. Examples include automatic isolation valves or remotely-operated motorised valves.

19.6.3.3 Defence in Depth Measures

In addition to the safety measures covered by Sub-claim_Flooding_2.2, other defence in depth measures are incorporated in the design:

a) In the UK HPR1000 plant design, pipes are not routed through electrical rooms or

I&C equipment rooms as far as practicable because the electrical or I&C equipment are vulnerable to flooding;

b) So far as it is reasonably practicable, pipes have been routed to minimise the number of rooms through which they pass;

c) Dry pipes for fire-fighting systems are preferred for installation in important rooms so that internal flooding effects of spurious operation or pipe failure of the fire-fighting systems on the SSCs required for delivering the safety functions are minimised；

d) Either a relocation of affected target equipment or removal of the flood sources from the potentially flooded rooms/ areas can be chosen to limit the consequences of internal flooding;

e) Where it is not possible either to limit the flooding level in a room or area or to qualify the SSCs for operation in a submerged environment, passive flooding mitigation design is used such that the flooding level does not submerge SSCs required for delivering the safety functions, for example, through placing SSCs on a pedestal/ platform.

19.6.3.4 Cliff Edge Effects

The cliff edge effects should be analysed to justify that there are no cliff edge effects in the UK HPR1000 internal flooding protection design. The analysis strategy of cliff edge effects for internal flooding is described as follows:

a) The sources considered in the internal flooding analysis are comprehensive. All systems and components containing liquid, except for HIC, are considered in the internal flooding analysis.

b) The maximum flooding level is calculated according to the worst case scenario of internal flooding. Gross failure is postulated for both high energy piping system and moderate energy piping system. The occupation by equipment in the room is considered in the flooding level calculation.

c) Margins are considered between the protection measures and calculation results. For example, the watertight doors for the lowest levels of the building are designed to withstand 10m hydraulic pressure (this value is larger than the largest basement height).

d) A sensitivity analysis of the flooding level is performed in the internal flooding assessment report. This is for determining that, for rooms in which the flood is released, the flooding level in case of high break flow rate does not challenge the boundaries of internal flooding zones.

19.6.4 High Energy Pipe Failures

19.6.4.1 High Energy Pipe Failures Introduction

The high energy pipe failures is identified as one of the major internal hazards in nuclear power plants. The high energy pipe failures can appear at any time during normal operation (e.g. power operation or shutdown). It is therefore important to ensure that high energy pipe failures would not prevent the delivery of fundamental safety functions.

According to Reference [9], the high energy pipes are defined as those pipes containing water or steam with pressure greater than or equal to 2MPa(g) under normal operating conditions, or with temperature no less than 100 ºC, or gas pipes pressurised above atmospheric pressure. The remaining pipes are defined as moderate energy pipes.

In the safety assessment of pipe failures, it is necessary to take into account the various effects of the postulated events in order to estimate the severity of the consequences. For high energy piping systems, their failures may cause both local effects and global effects. For moderate energy piping systems, only global effects are considered.

a) Local effects

   1) Pipe whip;

   2) Jet impingement;

   3) Blast wave.

b) Global effects

   1) Flooding;

   2) Overpressure due to steam release;

   3) Other effects (e.g. increase in temperature, humidity, radiation).

Pipe whip, jet impingement and overpressure due to steam release are considered in Sub-chapter 19.6.4. Blast wave is described in Sub-chapter 19.6.2 addressing internal explosion. Flooding is described in Sub-chapter 19.6.3 addressing internal flooding. Other effects resulting from high energy pipe failures (e.g. increase in temperature, humidity and radiation) will be considered in the qualification process for equipment if hazard consequences are unacceptable.

19.6.4.2 High Energy Pipe Failures Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence regarding the high energy pipe failures.

Sub-claim_HEPF_2.1: The high energy pipe failures sources are sufficiently identified.

Argument_HEPF_2.1.1: Gross failure is deterministically assumed to occur for all high energy pipes, except for pipes designed as high integrity component.

The list of high energy pipes is identified firstly according to the definition given in Reference [9]. High energy pipe failures are deterministically assumed to occur as gross failures (i.e. double ended guillotine break), except for HIC components which are justified in Chapter 17.

The assessment of high energy pipe failures is dependent on their break locations. Both terminal ends and intermediate points are considered as break locations according to mechanical calculation. Other locations representing bounding consequences are also considered.

Sub-claim_HEPF_2.2: After undertaking the safety assessment, the safety measures to mitigate the consequences of high energy pipe failures are sufficiently identified and properly classified.

Argument_HEPF_2.2.1: In segregation areas, the consequences of any high energy pipe failures are limited to one train of the systems delivering the safety functions through use of barriers.

After identifying the high energy pipes and determining the break locations, the consequences analysis is carried out according to *High Energy Pipe Failures Safety Evaluation Methodology Report*, Reference [27].

In segregation areas of the UK HPR1000, the principal protection features to protect systems delivering safety functions from the effects of high energy pipe failures are barriers. Redundant components are arranged in segregated divisions. Pipe whip and jet impingement are local effects and their consequences are limited to one division due to the barriers. The barriers segregating neighbouring divisions are designed to withstand the loadings induced by various effects of high energy pipe failures. The loss of one safety division is considered to be acceptable. The loading induced by high energy pipe failures will be determined. The barrier substantiation is presented in Chapter 16.

Compartment pressurisation due to steam release is a global effect due to high energy pipe failures. It results in distributed loads upon the associated barriers. The magnitude of pressurisation is associated with the rate of mass and energy release, the volume of the compartment, and the venting capability of the compartment. Relief devices are used in the UK HPR1000 to control compartment pressure where unmitigated effects may challenge the integrity of the barriers. Relief devices are passive devices that can be opened when the pressure reaches the specific threshold and the relief of the pressure is achieved.

Argument_HEPF_2.2.2: Where there are exceptions to segregation, consequences of high energy pipe failures can be restricted through additional safety measures (e.g. shields, restraints, geometrical separation) so as to ensure the delivery of the safety functions.

Exception to segregation areas are not reasonably practicable to divide with divisional barriers. The consequences of high energy pipe failures in exception to segregation areas are assessed to determine the shortfalls.

The main exception to segregation areas are in the BRX, the MCR and the VVP [MSS]/ ARE [MFFCS] pipes room in the BSB. The deterministic assessment will be carried out to assess the consequences of high energy pipe failures in these areas.

If the consequences of postulated high energy pipe failures are unacceptable, the dynamic effects may be restricted through the design of shields, restraints or geometrical separation. The application of these protection measures results in a restrained influence zone, which decreases the extent of the dynamic effects of pipe movement. Furthermore, the layout design is to be modified, e.g. locating systems and components important to safety away from high energy pipes, to avoid unacceptable consequences due to high energy pipe failures.

Argument_HEPF_2.2.3: The safety measures to mitigate the consequences of high energy pipe failures are classified according to certain criteria in line with the methodology of safety categorisation and classification.

Barriers provided to limit the effects of high energy pipe failures within the design basis are classified according to certain criteria in line with the *Methodology of Safety Categorisation and Classification,* Reference [22].

In addition, if additional protection measures (e.g. shields or restraints) are credited in the safety case, they are properly classified. In the UK HPR1000 design, according to Reference [22], functions provided to limit the effects of internal hazards within the design basis are categorised on the basis of the consequences of failure. For example, if the effects of high energy pipe failures cause the loss of a required FC1 safety function, the safety measures necessary to mitigate the effects of high energy pipe failures are to be classified as F-SC1.

Argument_HEPF_2.2.4: Where required, SSCs important to safety are capable to operate following a high energy pipe failure in the resulting environmental conditions.

SSCs important to safety are designed to operate in different environmental conditions. It is assumed that non-qualified SSCs are affected by the environmental consequences of a high energy pipe failure event and lose their functions. In the event the loss of equipment is unacceptable, the qualification process for equipment is carried out to ensure that components within rooms are qualified for resulting conditions of a high energy pipe failure event.

Sub-claim_HEPF_2.3: The safety measures to mitigate the consequences of high energy pipe failures are sufficiently substantiated.

Argument_HEPF_2.3.1: Barriers have the capability of withstanding the loading imposed by high energy pipe failures.

The barriers to deliver the protection against high energy pipe failures will be sufficiently substantiated. The loads resulting from the gross failure of high energy pipes include loadings induced by internal flooding, high temperature and overpressure, jet impingement and pipe whip, etc. The design of the concrete structure barrier adopts the finite element analysis method for barrier substantiation. The loads induced by high energy pipe failures are applied to the structure according to the static load, and the load combination is carried out in accordance with ACI 349-13, Reference [15], to check the bearing capacity of the structure.

19.6.4.3 Defence in Depth Measures

In addition to the safety measures covered by Sub-claim_HEPF_2.2, additional defence in depth measures are incorporated in the UK HPR1000 design:

a) High energy pipes are designed in accordance with appropriate rules;

b) The number of welds in high energy pipes is minimised as far as reasonably practicable (e.g. using bends instead of elbows);

c) Inspection of the high energy pipes can help early detection of leaks and initiation of subsequent operator actions;

d) The high energy pipes are arranged away from SSCs important to safety as far as reasonably practicable;

e) Where appropriate additional pipe restrains or shields are provided.

19.6.4.4 Cliff Edge Effects

The cliff edge effects should be analysed to justify that there are no cliff edge effects in the protection against high energy pipe failures in the UK HPR1000. The analysis strategy of cliff edge effects for high energy pipe failures is described as follows:

a) The sources identified in the high energy pipe failures analysis are comprehensive. All high energy pipes need to be analysed to demonstrate that consequences are acceptable.

b) Conservative calculation models and coefficients are used in high energy pipe failure safety assessments.

c) Deterministic assessments consider the worst case of high energy pipe failures. Gross failure and a single failure event (random failure) are deterministically assumed for all high energy pipes.

d) Margins are considered between the protection measures and calculation results.

19.6.5 Dropped Loads

19.6.5.1 Dropped Loads Introduction

Drops have the possibility to occur due to collapsed structures, falling objects and dropped loads. In this sub-chapter, dropped loads are considered, and the consequences of collapsed structures and falling objects are assessed as follows:

a) According to *NS-TAST-GD-014*, Reference [28], structures present at a nuclear site will be conservatively designed against severe hazards to an appropriate level commensurate with their consequence of failure. Therefore it is to be expected that the risk of a structural collapse will be low. So for collapsed structures, only if the structures of buildings are non-seismically classified, the risk of collapsed structures is considered. For the UK HPR1000, the buildings important to safety are all seismically classified. The design requirements of seismically classified buildings are provided in Chapter 16. However, there are some structures not seismically classified, such as masonry. The collapse of these structures will be identified and taken into account in earthquake safety assessments. Further methodology information is given in Reference [29].

b) For falling objects, if heavy items of plant equipment are located at significant heights, the possibility of dropping should be considered. For the UK HPR1000, if items important to safety are seismically classified, their falling is prevented under design basis earthquake; if not, the risk is identified and taken into account in the earthquake safety assessments. For seismically classified lifting devices, their falling can be prevented due to the following aspects:

    1) Seismically classified lifting devices are designed to satisfy the requirements of ASME-NOG-1 (presented in Sub-chapter 10.3);

    2) Mechanical structures of seismically classified lifting devices and its supporting components have sufficient strength to prevent collapse. The mechanical structures and the supporting components can maintain integrity under different kinds of design basis conditions to avoid dropping from the lifting devices;

    3) Seismically classified lifting devices are designed to support loads under design basis earthquake.

Dropped loads presented in this sub-chapter are assumed to occur as a result of failure of a lifting device (e.g. the lifting devices can no longer control the loads). Impacting loads are included in the dropped loads safety assessment, since they result from load swing or operating errors and they are defined as collisions of the loads with components or structures during handling. Dropped loads may be caused by operator error, random failure of components, overloads, etc. It may cause damage to the equipment and structures located under or in proximity to the lifting area.

19.6.5.2 Dropped Loads Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence of the dropped loads hazard.

Sub-claim_Dropped_2.1: The dropped loads sources are sufficiently identified.

Dropped loads are deterministically assumed to occur as a result of a lifting device failure (i.e. overload or sling break). In the UK HPR1000, the design requirements of lifting devices are detailed in Chapter 10. All of the lifting devices in the building important to safety are conservatively considered as sources of dropped loads even though the lifting devices are designed with high standards.

Dropped loads can be initiated by:

a) Failure of lifting devices used for fuel handling in BRX and BFX, which may result in damage of fuel assemblies and radioactive release, which is described in accident analysis (see Chapter 12);

b) Failure of lifting devices used for radioactive waste handling which are in BWX and BNX, which may not impact F-SC1/ F-SC2 items but may impact the radioactivity containment;

c) Failure of lifting devices used for other handling activities (e.g. maintenance) which may impact F-SC1/ F-SC2 equipment.

The most significant lifting actions include removal of the Reactor Pressure Vessel (RPV) head using the polar crane during the refuelling outage and lifting of the spent fuel cask using the spent fuel transport crane. In the T-19.6-3, bridge cranes in BRX/ BFX are listed considering the dropped loads consequences.

T-19.6-3 List of Main Lifting Devices

Buildings	Lifting device	Main lifting objects
Reactor Building	Polar crane	RPV head
		Upper internals
		Lower internals
		Multi-stud tensioning machine
		Reactor coolant pump and the motor
		Cavity cover slabs

Buildings	Lifting device	Main lifting objects
	Refuelling machine	Fuel assembly
		Control rod drive shaft
Fuel Building	Spent fuel cask crane	Spent fuel cask
	Spent fuel pool crane	Fuel assembly
		Spent Rod Cluster Control Assembly (RCCA)
	Auxiliary crane	New fuel transport container
		New fuel assembly
		Spent fuel transport cask cover
		Water gate

Sub-claim_Dropped_2.2: After undertaking the safety assessment, the safety measures to mitigate the consequences of dropped loads are sufficiently identified and properly classified.

Argument_Dropped_2.2.1: In segregation areas, divisional barriers are used to ensure that the consequences of any dropped load are limited to one train of the systems delivering the safety functions.

Systems delivering safety functions are arranged in the segregated buildings could ensure dropped load consequences limited to a single train. The divisional barriers segregating neighbouring divisions are such that the consequences of dropped loads in one division cannot prevent equipment in neighbouring divisions delivering their safety functions.

Argument_Dropped_2.2.2: Where there are exceptions to segregation, functional analysis is carried out to identify the safety measures to ensure sufficient SSCs are available, during and after dropped loads, to deliver the safety functions.

In areas that are exceptions to segregation where equipment belonging to different trains is not reasonably segregated by barriers, e.g. Reactor Building, a functional analysis is carried out to ensure that the consequences of dropped loads are acceptable.

The protection against dropped loads in the design of UK HPR1000 includes:

a) Redundant equipment important to safety is separated by sufficient distance to ensure an individual dropped load cannot directly impact two or more divisions;

b) The loads are required not to be carried over or near equipment important to safety or irradiated fuel, ensured through interlocks or layout design.

In the Reactor Building, the consequences of dropped loads are generally confined to a single train because drops are localised. But for the lifting of the RPV head during outage, the RPV head is removed and placed in a set down area. If it accidentally drops, this could potentially cause extensive damage to structures and the reactor. The consequences of such a drop will be assessed in GDA step 3.

In the BFX, the design of lifting devices and the lifting routes for fuel handling is described in Chapter 28. The radiological consequences of the spent fuel or spent fuel cask drop are described in Chapter 12.

In addition, it is necessary to carry out the dropped loads assessment for the lifting devices. Dropped loads are assessed on a case-by-case basis to ensure that they do not affect the safety functions, and the detailed analysis method can be found in Reference [30]. The assessment determines the following elements:

a) Identification of sources;

b) Identification of targets;

c) Functional analysis;

d) Protection measures if the consequences are not acceptable.

After safety assessment, measures are sufficiently identified and properly classified. The safety measures include protection and mitigation measures incorporated in the UK HPR1000 plant design.

Argument_Dropped_2.2.3: The safety measures to mitigate the consequences of dropped loads are classified according to certain criteria in line with the methodology of safety categorisation and classification.

Safety measures provided to limit the effects of internal hazards within the design basis are classified on the basis of the consequences of failure. For example, if the effects of dropped loads cause the loss of a FC1 safety function, safety measures necessary to protect against dropped loads are classified as F-SC1.

The passive safety measures, such as structures/ walls/ floors, are to protect systems from the effects of internal hazards and to limit any consequences of internal hazards. If there is redundant equipment in the upper and lower floors in the affected area of the dropped loads and the consequences analysis is unacceptable, reinforcing or thickening the floor can protect the equipment in the lower room from the effects of dropped loads.

Other safety measures include modifying the layout and modifying the lifting procedure, etc. If there is redundant equipment in the affected area of lifting device and the consequence analysis is unacceptable, one division of the redundant equipment can be moved out of the affected area. Modifying the lifting procedure, such as reducing the lifting height and separating the loads into smaller parts can minimise the effects of the dropped loads on structures. Rerouting the lifting paths can be also used to avoid the unacceptable condition if redundant equipment is located in the affected area.

Sub-claim_Dropped_2.3: The safety measures to mitigate the consequences of dropped loads are sufficiently substantiated.

Argument_Dropped_2.3.1: The floors can withstand the impact of dropped loads and cannot fail in the event of a dropped load.

Floor slabs can withstand dropped loads to protect the equipment on the lower floors. The heaviest load for one lifting device is selected to demonstrate the robustness of the barriers against dropped loads, based on the most onerous lift, by weight or by volume.

For structures, calculations are used to determine whether dropped loads can damage the structure or not and to determine the types of the damage (perforation, spalling, etc.). If the calculation shows that the structures are damaged, the equipment in the rooms below is also considered as a potential target to be damaged by dropped loads.

In the UK HPR1000, the only lifting device which operates above the Spent Fuel Pool (SFP) is spent fuel pool crane. The lifted loads handling by spent fuel pool crane are fuel assemblies and spent RCCA. Safety assessments will be performed to demonstrate that the SFP steel liner cannot be perforated by a dropped fuel assembly with handling tool attached. For the drop of the spent fuel cask and RPV head which are handled in the BFX and BRX respectively, calculations or simulation will be carried out to show the impact on structures.

Argument_Dropped_2.3.2: Divisional barriers can withstand the impact of dropped loads.

Divisional barriers may be impacted by dropped loads because of possible load swinging or tipping over. The assessment of dropped loads effects on divisional barriers will be carried out as necessary.

Argument_Dropped_2.3.3: Validation of lifting procedure execution and lifting route planning can contribute to avoiding unacceptable consequences highlighted by the safety assessment.

If the primary assessment of dropped loads shows that the consequences are unacceptable, the lifting procedure and route planning can be executed to mitigate the consequences of dropped loads. Lifting routes are re-designed such that the potential drops on equipment important to safety are avoided where possible and the lifting heights are reduced to limit the dropped loads effects on structure.

19.6.5.3 Defence in Depth Measures

In addition to the safety measures mentioned above, other defence in depth measures are incorporated in the UK HPR1000 design. It includes the following:

a) The probability of dropped loads is minimised in the following reasonably practicable ways:

1) Using appropriate design codes for lifting devices design (presented in Sub-chapter 10.3);

2) Meeting the requirements of single failure-proof design so far as is reasonably practicable;

3) By periodic inspection and early detection of incipient failure;

4) Performing operational procedures and operator training to reduce human error.

b) The consequences of dropped loads are minimised in the following reasonably practicable ways:

1) Minimising the travel and stoppage times above equipment important to safety and minimising the duration of the lift;

2) Minimising the speed and range of horizontal movements to limit the effect of swinging loads;

3) Defining a safe lifting route to reduce/remove the possibility of impacting items important to safety;

4) Providing interlocks to restrict movement of cranes over certain areas in certain modes of operation;

5) Providing single straight-line movements of the crane for all major lifts.

19.6.5.4 Cliff Edge Effects

The cliff edge effects are analysed to justify that there is no any cliff edge effects in the UK HPR1000 dropped loads protection design. The cliff edge effects can be minimised through the following aspects:

a) Deterministic assessment considers the worst case of dropped loads which takes into account the heaviest load and the highest height, etc.;

b) The equipment in the affected area of dropped loads is assumed to be unavailable, and the parameters selected for the calculation of the impact of dropped loads on structures are conservative;

c) There are sufficient safety margins between the calculation result and the acceptance criteria;

d) The assessment adopts deterministic approaches which are conservative in both analysis hypothesis and methodology.

19.6.6 Internal Missiles

19.6.6.1 Internal Missiles Introduction

The internal missiles is identified as one of the major internal hazards in nuclear power plants. Internal missiles may be generated by rotating machinery and high energy fluid system equipment failure.

As defined in *Internal Missiles Safety Evaluation Methodology Report*, Reference [31], the typical internal missiles sources that have been considered are as follows:

a) Internal missiles from rotating equipment failures, including pumps, fans, compressors, motors, turbines, etc.;

b) Internal missiles from high energy fluid system equipment failures, including vessels, valves, control rod drive mechanism, etc.

19.6.6.2 Internal Missiles Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence made regarding the internal missiles hazard.

The delivery of safety functions is shown to be ensured through a combination of the following claims, arguments and evidence with regards to internal missiles.

Sub-claim_Missiles_2.1: The internal missiles sources are sufficiently identified.

Argument_Missiles_2.1.1: Equipment is identified as potential internal missiles sources regardless of its classification except for equipment designed as high integrity component.

In practice, the safety classification of SSCs in the UK HPR1000 can provide a systematic method for classifying equipment into different levels of design code in line with its safety class, the consequences of its failure and protection.

In general, the reliability and robust quality of design and manufacture of equipment are ensured through meeting the requirements of codes and standards which are commensurate with the safety class of components.

For internal missiles assessment, equipment is conservatively identified as potential internal missile sources regardless of its classification, although the probability of equipment meeting certain classification requirements to become an internal missile source is low.

HIC components, whose failure frequency is extremely low and the failure consequences are unacceptable, are identified based on the results of failure consequences analysis, and need to meet additional requirements. The HIC components are manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained in accordance with the established design requirements and the appropriate levels of quality and safety requirements to ensure its structural integrity and are not considered as internal missile sources.

Argument_Missiles_2.1.2: Although the probability of failure of an essential SSC due to turbine missiles is extremely low, turbine missile has been identified as potential internal missile source and assessed in both deterministic and probabilistic approaches.

In the specific case of turbine disintegration, in view of the large mass of the impellers and high rotational speed (1500 rpm), in the unlikely event of impeller disintegration, the missile pieces would have significant energy which could potentially cause damage to buildings in their flight path. The turbines have been orientated within the Turbine Building such that the most likely direction of the missiles would not coincide with the location of the buildings important to safety. However, it is still possible that a missile piece(s) could be directed towards key buildings (albeit with very low probability). The assessment of turbine disintegration to be undertaken in GDA step 4 will consider this possibility to determine if any credit can be taken for 'structures' in the missile path (turbine casing, Turbine Building structure and impacted building structure). Both deterministic and probabilistic assessment supports the overall safety case.

According to *RG1.115*, Reference [13], the generated energetic missiles are usually ejected within a very narrow angle of the plane of rotation, so the turbine should be appropriately orientated such that the most likely direction of the missiles would not coincide with the location of the main nuclear buildings. F-SC1/ F-SC2 SSCs should not be located in the cone area bounded by lines that are inclined within 25 degrees to the turbine wheel planes.

For the area beyond the 25 degrees range, cliff edge effects will be analysed, taking into consideration wider direct strike angles.

Sub-claim_Missiles_2.2: After undertaking the safety assessment, the safety measures to mitigate the consequences of internal missiles are sufficiently identified and properly classified.

With regards to internal hazards, there are two categories of areas: one is areas with segregation and the other is exception to segregation areas. Argument_Missiles_2.2.1 and Argument_Missiles_2.2.2 presented below indicate how the internal missiles are mitigated within these two categories.

Argument_Missiles_2.2.1: In segregation areas, safety measures are identified to ensure that the consequences of any internal missile are limited to one train of the systems delivering the safety functions through use of barriers.

The redundant equipment of F-SC1/ F-SC2 systems is arranged in segregated divisional compartments (segregated buildings such as Safeguard Buildings). This ensures that the internal missiles can be limited in a single division.

The barriers associated with these divisional compartments are designed to provide the principal means to ensure that the internal missile will be contained within a single division. These hazard barriers are substantiated to withstand any internal missile impact around this area. The acceptance criteria can be no perforation of the barrier, and preferably no scabbing on the other side unless it can be demonstrated that there are no SSCs important to safety potentially impacted on the other side in the adjacent room (different division), or the functional analysis result is acceptable.

Argument_Missiles_2.2.2: Where there are exceptions to segregation, safety measures are identified to ensure that sufficient SSCs are available, during and after an internal missile, to deliver the safety functions.

It is necessary to carry out the internal missiles safety assessment for the areas where there are exceptions to segregation to identify the safety measures.

The assessment is based on the approach outlined in Reference [31], including demonstrating sufficient separation and taking credit for local protection measures, including the local internal missile partitions, and enhancing the impacted boundary.

Argument_Missiles_2.2.3: The safety measures to mitigate the consequences of internal missiles are classified according to certain criteria in line with the methodology of safety categorisation and classification.

Safety measures provided to limit the effects of internal hazards within the design basis are classified on the basis of the consequences of failure.

For passive safety measures, such as structures/walls, their main function is to protect systems from the effects of internal hazards and to limit any consequences of internal hazards. The classification of structures/walls should be consistent with classes of the protected systems. The safety measures required to protect SSCs from internal missiles that could result in loss of a required FC1 safety function are classified as F-SC1; the safety measures required to protect SSCs from internal missiles that could result in loss of a Category 2 (FC2) safety function are classified as Class 2 (F-SC2).

Sub-claim_Missiles_2.3: The safety measures to mitigate the consequences of internal missiles are sufficiently substantiated.

Argument_Missiles_2.3.1: Barriers between different divisions are substantiated to withstand the loading imposed by internal missiles.

Argument_Missiles_2.3.2: Walls/ floors/ additional local partitions which are claimed to have the function of internal missile protection are also substantiated to withstand the loading imposed by internal missiles.

Barriers between different divisions are designed to withstand the loading imposed by internal missiles. Calculations are carried out to demonstrate the substantial capacity of these barriers against internal missile impacting them.

Besides divisional barriers, walls/ floors/ additional local partitions also have the capacity to protect internal missiles and in some cases, they are claimed as local internal missile partitions. For these structures, calculations are also carried out to demonstrate the bearing capacity of these local partitions against the internal missile impacting them.

The claimed barriers and local partitions have sufficient bearing capacity and anti-penetration capacity.

In designing the structural members used to resist the impact of missiles, penetration effect, back spalling effect and other effects are assessed predominantly on the basis of empirical formulas. The selection of the empirical formulas will depend on the parameter of the missiles.

19.6.6.3 Defence in Depth Measures

In addition to the safety measures covered by Sub-claim_Missiles_2.2, other defence in depth measures are incorporated in the design:

a) Measures are taken to minimise the possibility of internal missiles occurrence.

Generally, the probability of the occurrence of internal missiles is reduced through using the appropriate design standards, specification of materials and equipment, carrying out strict quality assurance requirements, quality control inspections during manufacture, operation and maintenance provisions. In addition, the probability of internally generated missiles is reduced through consistent application of safety orientated design and engineering principles.

For pressure-containing components of a high energy fluid system, such as valves or containers, conservative design, high quality manufacturing, rigorous testing, careful operation, proper monitoring of parameters (such as vibration) and comprehensive in-service inspection contribute to preventing them from becoming credible internal missile source.

High-speed rotating pumps or fans normally have a strong enough shell to ensure that the blade missiles can be contained or the energy of the missiles can be significantly reduced. Meanwhile, as a standard measure, high-speed rotating machinery is always equipped with over-speed protection systems which contribute to preventing them from becoming a credible internal missile source or effectively reduce the energy of potential missile.

b) For the layout design, redundancy and segregation are considered in the arrangement of items important to safety to avoid any potential threat from internal missiles;

c) Valve installation direction ensures that the valve stems or the valve bonnet missiles do not affect the F-SC1/ F-SC2 SSCs as far as possible;

d) Over-speed prevention, detection and alarm devices are considered in the design of rotating machinery.

19.6.6.4 Cliff Edge Effects

The cliff edge effects should be analysed to justify that there are no cliff edge effects associated with internal missiles protection design for the UK HPR1000. The protection design against internal missiles is based on a conservative approach with appropriate margins which can be used to improve resilience against cliff edge effects. Therefore, the analysis strategy of cliff edge effects for internal missiles is described as follows:

a) The sources considered in the internal missiles safety assessment are comprehensive and conservative. The internal missiles safety assessment scope covers all potential internal missile sources which may impact SSCs important to safety within the plant except for equipment designed as HIC;

b) Meanwhile, a comprehensive assessment is undertaken for design basis internal missiles for each building containing SSCs delivering safety functions. The assessment adopts deterministic approaches which are conservative in both analysis hypothesis and methodology;

c) Conservative approaches are used in the calculation of characteristic parameters of the potential missiles, the substantiation of barriers and the consequences assessment. For example, for the consequences assessment of internal missiles, all the equipment located in the missile impact range is conservatively considered to be lost.

19.6.7 Electromagnetic Interference (EMI)

19.6.7.1 EMI Introduction

EMI is a term used to describe a number of potential disturbance mechanisms with the potential to affect electrical or electronic devices caused either by electromagnetic induction or by electromagnetic radiation. As the sensitive I&C components or electronic equipment might be affected by the effects of EMI, EMI is identified as one of the internal hazards that must be considered in nuclear power plants design. EMI originating offsite is addressed in Chapter 18. This section is focussed on EMI originating on-site (internally generated electromagnetic interference).

EMI may be generated by induction or radiation from installed equipment, either in normal operation or in fault conditions, such as:

a) Switchgears;

b) Circuit breakers or fuses;

c) Variable speed drives.

EMI can also be generated by maintenance or construction/operation activities, such as:

a) Welding operations;

b) Portable radio communications.

19.6.7.2 EMI Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence made regarding the EMI hazard.

Sub-claim_EMI_2.1: The safety measures to mitigate the consequences of EMI are sufficiently identified.

EMI behaves differently from other internal hazards as it could interfere directly with I&C equipment or electronic equipment and may not be readily stopped by physical hazard barriers which are used to provide protection from other internal hazards. So the safety measures to mitigate the consequences of EMI have some differences from those used for other hazards.

Argument_EMI_2.1.1: Isolation measures are adopted as they can have a significant effect on reducing the pervasiveness of the EMI hazard.

In the plant layout design, as a general requirement, for the arrangement of sensitive electrical and I&C equipment, cable trays, cabinets and components, no significant EMI source is allowed to be located within adjacent areas.

As a general requirement, I&C signal cables are isolated from power cables. They are routed in different cable trays and have appropriate separation from each other to ensure that the signal cables will not be affected by the EMI generated by power cables to avoid spurious signals.

Argument_EMI_2.1.2: Shielding measures are adopted as they can have a significant effect on reducing the pervasiveness of the EMI hazard.

Shielding of equipment and cables from sources of magnetic and electromagnetic radiation is a common measure to be taken in the protection against EMI.

The cabinets can provide a certain degree of protection against EMI effects for the I&C components/equipment inside.

Cable trays for sensitive I&C signal cables are always equipped with steel covers to provide protection against EMI effects.

Argument_EMI_2.1.3: Electronic and Instrumentation and Control (I&C) equipment is designed and qualified to reduce the susceptibility to EMI effects.

Information of design and qualification requirements of sensitive electronic and I&C equipment to reduce the susceptibility to EMI effects can be found in Chapter 8 Instrumentation & Controls.

Further measures can be taken, such as filtering electromagnetic noise before it can affect sensitive electronic circuits to reduce the susceptibility to EMI effects; and proper grounding of electrical and I&C equipment, raceways, cabinets, components and cable shields, etc.

Sub-claim_EMI_2.2: The safety measures to mitigate the consequences of EMI are sufficiently substantiated.

As EMI behaves differently from other internal hazards, it is hard to directly quantify its effects and substantiate the safety measures in a conventional approach but it is essential to prove that the EMI environment in which the sensitive I&C components or electronic equipment are located in is acceptable.

For example, the I&C system is tested and substantiated, including undertaking conducted emission testing, radiated emission test, harmonic immunity of alternating current power lines testing, etc. These tests are used to prove the substantiation of the safety measures provided for these systems and components for EMI protection can ensure that the EMI environment for these sensitive components will not lead to unacceptable consequences.

19.6.7.3 Defence in Depth Measures

In addition to the safety measures mentioned above, other defence in depth measures are incorporated in the design:

a) Measures are taken to minimise the EMI sources. As a general requirement, the potential EMI source equipment is designed and qualified according to appropriate standards and to suppress electromagnetic noise to an appropriate level.

b) The correct operation of the systems depends on ensuring that the electromagnetic environment within which electrical and electronic systems operation is controlled to be within acceptable limits.

c) There are also strict administrative control measures for EMI sources. For potential temporary EMI sources being introduced by maintenance or construction activities, concerning the usage of portable communication devices such as mobile telephones or radios and welding operations, there are strict administrative control measures (such as access arrangements, warning notices, work control systems) to prevent them from becoming credible EMI sources. Also, for potential temporary EMI sources, there are restriction requirements on portable electronic devices near sensitive equipment. For welding operations, they are only permitted in specific areas and during specific operational periods.

d) Meanwhile, building structures (walls and floors) which behave in a similar manner to a Faraday cage, can also provide a degree of protection against EMI propagation due to their metal structures.

19.6.7.4 Cliff Edge Effects

The cliff edge effects should be analysed to justify that there are no cliff edge effects in the design of protection against EMI. The analysis strategy for EMI-related cliff edge effects for the UK HPR1000is described as follows:

a) The sources considered are comprehensive and conservative. EMI protection design scope covers all potential EMI sources which may impact SSCs important to safety within the plant;

b) Meanwhile, for the design, manufactory and test of the sensitive electrical and I&C equipment, cable trays, cabinets, components, margins are always provided to ensure that they have sufficient capability to withstand the EMI electromagnetic environment where they are located.

19.6.8 Toxic and Corrosive Materials and Gases

19.6.8.1 Toxic and Corrosive Materials and Gases Introduction

This sub-chapter addresses the hazards originating from a release of toxic and corrosive materials and gases that are stored within the site boundary.

Toxic and corrosive materials and gases have the potential to disable both items important to safety and personnel carrying out actions important to safety, through the following effects:

a) Toxic effects. The toxic effects caused by release of hazardous sources could be fatal to personnel and thus disable personnel carrying out actions important to safety;

b) Corrosion effects. Release of corrosive materials could cause corrosive effects on SSCs important to safety. However, corrosive effects on SSCs are considered as a slow process which takes time to reveal itself. Therefore, it is considered that SSCs will not be disabled in the short-term;

c) Asphyxiation effects. Release of materials with strong volatility or release of anoxic gases in a room could cause reduction to the amount of oxygen and thus asphyxiate personnel.

19.6.8.2 Toxic and Corrosive Materials and Gases Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence made regarding the toxic and corrosive materials and gases hazard.

The following claims, arguments and evidence are focused on preventing items important to safety or personnel carrying out actions important to safety from the effects of releases of toxic and corrosive materials and gases.

Sub-claim_Toxic_2.1: The toxic and corrosive materials and gases sources are sufficiently identified.

The tanks and vessels in which the hazardous materials are stored are designed in accordance with appropriate codes. However, the deterministic assessment of toxic and corrosive materials and gases cannot preclude their release. And the sources are sufficiently identified. The information on chemical substances to be used on the UK HPR1000 is provided in Reference [32]. During GDA phase, the quantity of each dangerous substance has not been fixed. Therefore the quantity of each dangerous substance is based on the values estimated from existing China General Nuclear Power Corporation (CGN) fleet feedback. It is noted that the quantity of each dangerous substance depends on operational decisions by operators at the site-specific stage.

There is only a very limited quantity of toxic and corrosive materials and gases stored and used within the nuclear power plants, including:

a) Bulk stored gases. Examples of these could be hydrogen, nitrogen and carbon dioxide. For the release of hydrogen, the effects can be covered in the frame of internal fire or internal explosion;

b) Bottled gases, if stored in sufficient quantities;

c) Volatile liquids that could evaporate. These could include releases of ammonium hydroxide and hydrochloric acid with strong volatility, which may affect personnel carrying out actions important to safety;

d) Chemicals used in water chemistry such as hydrazine, sodium hydroxide, hydrochloric acid and nitric acid.

Sub-claim_Toxic_2.2: The release of toxic and corrosive materials and gases does not cause the loss of the safety functions.

The safety assessment for the release of toxic and corrosive materials and gases will be carried out based on the following steps:

a) Identify the list of potential sources including their characteristics (i.e. quantity, physical and chemical properties, type and storage locations);

b) Assess the potential consequences on equipment or personnel in the event of release of these sources;

c) Identify safety measures necessary to protect personnel carrying out actions important to safety and protect SSCs important to safety against the effects of toxic and corrosive materials and gases.

Argument_Toxic_2.2.1: The MCR remains habitable in the event of a release of toxic and corrosive materials and gases.

More attention is paid to the MCR because personnel are required to carry out actions important to safety during normal operation and even in accident conditions. As is stated in Sub-chapter 19.4, the safety objective is to ensure the habitability of the MCR in every individual hazard or credible hazard combinations.

The MCR operators could be impeded to carry out actions important to safety by a release of toxic and corrosive materials and gases which could reach the MCR. Corrosive liquid cannot enter the MCR because the MCR is included in a forbidden internal flooding zone (see Sub-chapter 19.6.3). The concentration of toxic gases in the MCR will be assessed qualitatively or quantitatively, and if necessary, protective measures will be determined.

The Main Control Room Air Conditioning System (DCL [MCRACS]) is designed to maintain the ambient conditions required for safety and the habitability of the MCR (see Chapter 10). The DCL [MCRACS] is required to operate during normal operation in recycling mode. The fresh air supply and associated equipment in operation, except the iodine filter, trains are safety classified. Air circulation in the MCR could mitigate the effects of releases of toxic substances.

Argument_Toxic_2.2.2: Sufficient systems are available, during the release of toxic and corrosive materials and gases, to deliver the safety functions.

The effects due to release of toxic and corrosive materials and gases should not affect the components important to safety and thus ensure the delivery of safety functions.

In the UK HPR1000 design, redundant trains of systems important to safety are located in different divisions. Where there is the potential for components important to safety to be affected by the effects due to release of toxic and corrosive materials and gases, redundant trains remain available to fulfil the safety functions.

For stored gases, none of them is corrosive and there is no challenge to component performance except for choking of diesel generators. However, different divisions of diesel generators are located in different buildings such that sufficient redundant diesel generators are unaffected by the release and that their safety functions will be successfully fulfilled even following failure of one diesel generator.

For liquid hazardous materials, there are both flooding effects and corrosion effects. Since the corrosion effects are gradual and action is taken to drain the corrosive liquid, it is considered that components will not be disabled in a short-term. The flooding effects are prompt and may disable components important to safety. In segregation areas, barriers are designed to limit the consequence to one train of the systems delivering the safety functions. Where there are exceptions to segregation, functional analysis is carried out to identify the safety measures to ensure sufficient components are available. It is described in Sub-chapter 19.6.3 addressing internal flooding.

Argument_Toxic_2.2.3: The safety measures to mitigate the consequences of Toxic and corrosive materials and gases release are classified according to certain criteria in line with the methodology of safety categorisation and classification.

The safety measures are classified according to certain criteria in line with the methodology of safety categorisation and classification, Reference [22]. According to Reference [22], functions provided to limit the effects of internal hazards within the design basis are categorised on the basis of the consequences of failure.

19.6.8.3 Defence in Depth Measures

In addition to the safety measures covered by the Sub-claim_Toxic_2.2, other defence in depth measures are incorporated in the design:

a) In the UK HPR1000 plant design, the location of permanently occupied areas such as control rooms and offices in relation to bulk storage of toxic and corrosive materials and gases should be chosen carefully;

b) The possibility of toxic gases entering ventilation systems and thereby affecting operators in the control room should be minimised;

c) To protect personnel against the effects of release of toxic gases, the main control room is equipped with protective masks and oxygen cylinders. Personnel can wear these protective measures if there are signs of release of toxic or harmful substances;

19.6.8.4 Cliff Edge Effects

The cliff edge effects should be analysed to justify that there are no cliff edge effects in the toxic and corrosive materials and gases protection design of the UK HPR1000. The analysis strategy of cliff edge effects for toxic and corrosive materials and gases is described as follows:

a) All hazardous substances within the site boundary are considered in toxic and corrosive materials and gases assessments.

b) Under the worst case ambient conditions, a release of toxic gas will not expose the personnel in the MCR to concentrations above the unacceptable level of toxicity. Concentration margin should be considered in the cliff edge effects analysis.

19.6.9 Vehicular Transport Impact

19.6.9.1 Vehicular Transport Impact Introduction

At nuclear installations material and equipment is moved using a variety of forms of transport. If the transport is not adequately controlled, there is a potential for impacts that could have implications for nuclear safety, Reference [28]. Thus vehicular transport impact needs to be considered as an internal hazard and assessed during GDA.

The vehicular transport impact assessment considers the effect of collision. Other consequential effects, such as fire and explosion, are considered in the corresponding internal hazards.

19.6.9.2 Vehicular Transport Impact Claims, Arguments and Evidence

This sub-chapter presents the claims, arguments and evidence made regarding the vehicular transport impact.

The delivery of safety functions is shown to be ensured through a combination of the following claims, arguments and evidence made on hazard barriers and the required protection and mitigation measures in the event of vehicular transport impact.

Sub-claim_Vehicle_2.1: The vehicular transport impact sources are sufficiently identified.
Argument_Vehicle_2.1.1: All the vehicles that can approach or enter the buildings important to safety are identified as vehicular transport impacts sources.
Argument_Vehicle_2.1.2: The vehicular transport impact sources are divided into two types according to the impact location: inside or outside the buildings important to safety.

Vehicular transport is unavoidable, particularly during outage periods. A full list of vehicles transporting onsite will be developed to support the assessment. Because of the different impact scenarios, vehicular transport impacts inside and outside the buildings important to safety are considered individually with different load cases.

Sub-claim_Vehicle_2.2: The safety measures to mitigate the consequences of vehicular transport impacts are sufficiently identified and properly classified.

Argument_Vehicle_2.2.1: Systems and components important to safety are protected from the vehicular transport impact outside the buildings.

Argument_Vehicle_2.2.1.1: The plant layout and transport route are well designed to avoid the consequence of vehicular transport impact outside the buildings.

In the UK HPR1000 design, systems or components important to safety are located inside the buildings (expect the silencers of Atmospheric Steam Dump System which are located on the roof of Safeguard Building). The *Scope for UK HPR1000 GDA Project*, Reference [17], gives the layout for UK HPR1000. The layout of UK HPR1000 can ensure that the main access routes are separated from the buildings important to safety by rail.

Argument_Vehicle_2.2.1.2: Structures of buildings important to safety have the capacity to withstand the load caused by vehicular transport impact outside the buildings.

As mentioned in Chapter 16, the structures of buildings important to safety are reinforced concrete and have been designed as resilient to loads from external hazards, such as aircraft impact and tornado generated missile. Such structures can provide a high degree of confidence that they can maintain their integrity and prevent vehicular transport impact form damaging systems and components important to safety housed inside.

Argument_Vehicle_2.2.2: Systems and components important to safety are sufficiently segregated and protected from the consequences of vehicular transport impact inside the building.

Argument_Vehicle_2.2.2.1: Vehicle access to buildings important to safety is limited to specific areas.

Vehicle access to buildings important to safety is limited to specific areas during outage. For the BRX, vehicle access is limited to BEX and the equipment is introduced into BRX through the equipment gate at +17.50m level. For the BFX, vehicle access is limited to the PMC transfer room which is completely segregated from other rooms by concrete walls. For other segregation buildings, during outages, only a single safety division will be out for maintenance and vehicle will only be able to access the entrance areas at the access level of that division.

Argument_Vehicle_2.2.2.2: Structures of buildings important to safety have the capacity to withstand the load caused by vehicular transport impact inside the building.

The external doors of buildings important to safety are normally closed. A vehicle to enter the buildings has to stop and wait for the doors to be opened. This procedure, along with site speed limits, ensures that the entering velocity is minimised (less than 10km/h). Thus the maximum velocity that a vehicle could achieve before impacting the structures would be low. Low velocity impact is not assumed to compromise the integrity of internal structures. The penetration effect of vehicles will be calculated.

Argument_Vehicle_2.2.3: The safety measures to mitigate the consequences of vehicular transport impact are classified according to certain criteria in line with the methodology of safety categorisation and classification.

Safety measures provided to limit the effects of internal hazards within the design basis are principally barriers.

The safety measures are classified according to certain criteria in line with the methodology of safety categorisation and classification, Reference [22]. According to Reference [22], functions provided to limit the effects of internal hazards within the design basis are categorised on the basis of the consequences of failure. For example, if the effects of a vehicular transport impact will cause the loss of a required FC1 safety function, the safety measures necessary to protect against vehicular transport impact are to be classified as F-SC1.

Sub-calim_Vehicle_2.3: The safety measures to mitigate the consequences of vehicular transport impacts are sufficiently substantiated.

Argument_Vehicle_2.3.1: Bounding case is used to qualify the ability of structures to withstand the load caused by vehicular transport impact outside the building.

Argument_Vehicle_2.3.2: Bounding case is used to qualify the ability of structures to withstand the load caused by vehicular transport impact inside the building.

The bounding case for vehicular transport impact will be conservatively determined, taking the velocity, mass, size, frequency and other factors into consideration. Because of the different scenario, the impact of vehicular transport inside or outside the buildings will be enveloped by different bounding cases.

The design of civil structures should take the load caused by vehicular transport impact into account. An assessment will be carried out based on the bounding case to demonstrate that the substantial capacity of these structures is sufficiently resilient against vehicular transport impact.

19.6.9.3 Defence in Depth Measures

In addition to the safety measures covered by the Sub-claim_Vehicle_2.2, other defence in depth measures are incorporated in the design.

Vehicular transport impact is typically due to human error. Therefor it is impossible to eliminate this kind of internal hazard from UK HPR1000 design. However, administrative measures can greatly reduce the probability of vehicular transport impact:

a) Vehicular transport impact source is minimised, only the approved vehicles are allowed to enter the site;

b) Vehicles transporting on site are subject to strict speed restrictions which are commensurate with the consequence of human error;

c) The drivers are well trained to operate the vehicle appropriately;

d) Operational procedure is made to control on site vehicular transport and more onerous operating restrictions are given for multiple vehicle movements.

In addition to the administrative measures, other design measures are available to mitigate the consequence of vehicular transport impact. For example, landscaping features design can also provide protection to buildings from vehicular transport impact.

19.6.9.4 Cliff Edge Effects

The cliff edge effects should be analysed to justify that there are no any cliff edge effects which can impact the delivery of safety functions. The UK HPR1000 analysis strategy for cliff edge effects for vehicular transport impact is described as follows:

a) The sources considered in the vehicular transport impact analysis are comprehensive. All potential vehicles on site are considered in the vehicular transport impact analysis;

b) The bounding cases are calculated according to the worst case scenarios of both vehicular transport impacts inside and outside the buildings (e.g. largest speed, heaviest vehicle, highest frequency, etc.);

c) Margins are considered between the protection measures and calculation results of the collision. For example, the structures of buildings important to safety are designed to withstand extreme loads resulting from external hazards which are potentially greater than those presented by vehicular transport impact.

19.7 Assessment of Hazard Combinations

Sub-chapter 19.6 describes the individual internal hazards, and this sub-chapter demonstrates that the consequences of the credible hazard combinations are acceptable or minimised by protection measures. Hazard combinations are considered as part of the hazard assessment to ensure that safety measures implemented are suitable and sufficient. This is because the effects of combined hazards have the potential to be superimposed or have delayed impacts and as a consequence exceed the limit of the available safety measures. The safety requirements of hazard combinations are consistent with those of the individual internal hazards mentioned in Sub-chapter 19.6.

For each identified hazard combination sequence, the analysis should also take into consideration any deterioration or damage to SSCs important to safety and hazard barriers after being subjected to each of the various hazards.

Sub-claim_Combination_2.1: After undertaking the safety assessment, the safety measures to mitigate the consequences of hazard combinations are sufficiently identified and properly classified.

For segregation buildings, it is conservatively assumed that an internal hazard will potentially result in the loss of all SSCs within the affected division, so any credible combined internal hazards which will affect the same segregated division will not impact the delivering of three fundamental safety functions.

For exception to segregation buildings, the assessment for credible combined internal hazards focuses on the potential damage of each internal hazard, to clarify whether the combined internal hazards could result in the loss of more than one train of the systems delivering the safety functions or not, and some essential protection measures will be applied to mitigate the consequence. The safety measures are classified according to certain criteria in line with the methodology of safety categorisation and classification, Reference [22].

The analysis assumption and hypothesis as applicable to each of individual internal hazard remains applicable to the assessment of combined internal hazards. The detailed internal hazard combinations safety assessment will be provided in corresponding internal hazards safety assessment reports.

Sub-claim_Combination_2.2: The safety measures to mitigate the consequences of hazard combinations are sufficiently substantiated.

The safety measures (except hazard barriers) to mitigate the consequences of hazard combinations should be substantiated using the same strategy as that which is used for individual internal hazards safety measures substantiation.

The design and qualification of hazard barriers against single internal hazard loads should be considered in the individual internal hazard safety assessment and barrier substantiation. However, the load combination due to the combined hazards could give more significant challenges to the hazard barrier design. The load combination should be considered in the civil structure design which is described in Chapter 16.

19.8 ALARP Assessment

As part of the ALARP demonstration presented in Chapter 33, the current ALARP assessment which will be developed throughout GDA for internal hazards protection design for the UK HPR1000 is presented in this sub-chapter.

19.8.1 General Approach for ALARP Assessment

Chapter 33 and its referenced document *ALARP Methodology*, Reference [33], present the generic approach of demonstrating that the risk is reduced to be ALARP in the design and operation. The ALARP assessment for internal hazards protection design applies this approach and consists of the following steps:

a) Identifying sources of RGP;

b) Analysing the RGP and applying a consistency review against RGP;

c) Identifying the gaps from step b) ;

d) Undertaking the internal hazards safety assessment and finding out potential enhancements;

e) Undertaking analysis of the ALARP options for the potential enhancements;

f) Selecting an optimal solution and implementation for potential enhancement.

19.8.2 Sources of RGP

A review of the sources of RGP is undertaken to help to identify suitable options to reduce risk. For the UK HPR1000, the sources of RGP applied to protect against internal hazards are identified. The sources of RGP predominantly come from the following aspects, in line with Reference [33]:

a) IAEA Safety Guidance;

b) Recognised Design Codes and Standards;

c) SAPs and Technical Assessment Guides (TAGs);

d) Regulator Expectations.

In addition, input from the regulator (e.g. Regulatory Observations (ROs), Regulatory Issues (RIs)) is considered as part of the process of identifying potential improvements. Additionally, ROs, RIs and GDA Issues from past GDAs are also considered.

The sources of RGP are listed in T-19.8-1.

T-19.8-1 Sources of RGP

No.	Title	Source	Remark
1	Safety Assessment Principles for Nuclear Facilities, SAPs, Revision 0, November 2014	ONR	For all internal hazards
2	NS-TAST-GD-014 Internal Hazards	ONR	For all internal hazards
3	NS-TAST-GD-056 Nuclear Lifting Operations	ONR	Dropped loads
4	NS-TAST-GD-081 Safety Aspects Specific to Storage of Spent Nuclear Fuel	ONR	Dropped loads
5	Safety Requirements: Safety of Nuclear Power Plant: Design, No.SSR-2/1, Revision 01, 2016	IAEA	For all internal hazards
6	Safety Guide NS-G-1.7. Protection against Internal Fires and Explosions in the	IAEA	Internal fires and

No.	Title	Source	Remark
	Design of Nuclear Power Plants, 2004		explosions
7	Safety Guide NS-G-1.11, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, 2004	IAEA	Chapter 1 and 2 of this guide is applicable for all internal hazards. Chapter 3 is applicable for all internal hazards except fire, explosion, EMI and toxic and corrosive materials and gases (This guide is currently being updated)
8	Safety Guide: Design of Fuel Handling and Storage Systems for Nuclear Power Plants, NS-G-1.4, 2003	IAEA	Dropped loads
9	Safety Reference Levels for Existing Reactors, September 2014	WENRA	For all internal hazards
10	Safety of New Nuclear Power Plant design, March 2013	WENRA	For all internal hazards
11	EPR Technical Code for Fire Protection, ETC-F 2010	AFCEN	Internal fire
12	The Dangerous Substances and Explosive Atmospheres Regulations, 2002 No.2776, 2002	Health and Safety	Internal explosion
13	Protection against Turbine Missiles, RG1.115, 2012	NRC	Internal missiles
14	Control of Heavy Loads at Nuclear Power Plants, NUREG 0612, 1980	NRC	Dropped loads
15	NRC, Standard Review Plan, NUREG	NRC	High energy pipe failures and

No.	Title	Source	Remark
	0800, 2007		internal flooding (Specifically Section 3.4.1, 3.6.1, 3.6.2, 3.6.3 and BTP 3-3, 3-4)

19.8.3 Consistency Review against RGP and Gap Analysis

The consistency review is carried out based on the requirements from RGP for the overall protection design against internal hazards. Some gaps have been identified at the current phase through a use of the consistency review against RGP.

However, the gap analysis is a continuous task during the whole GDA process. Further efforts will be made during GDA step 3 and step 4 for those gaps on the design of UK HPR1000 to eliminate those gaps and to demonstrate that the risk is reduced to ALARP, according to the different steps described in 19.8.1.

19.9 Concluding Remarks

The protection design and safety assessment guarantee that the internal hazards do not compromise safety functions. This is ensured primarily by incorporating robust hazard barriers, such that generally only one division of safety systems that deliver the safety functions will be potentially lost, and the redundant systems (i.e. other divisions) will remain fully available. The hazard barriers are designed to withstand the loads from any individual (or credible combination) design basis hazard. The design is based on conservative calculation approach. This will ensure that any abnormal (beyond design basis) load is unlikely to result in a cliff edge effect. In addition, ‘defence in depth’ measures that prevent the occurrence of internal hazards and protect SSCs important to safety from the effects of internal hazards have been incorporated in the design.

During GDA step 3 and step 4, further analysis will be performed to confirm that the safety functions for the UK HPR1000 will be available during design basis internal hazards. In addition, at the current phase, some gaps have been identified and further efforts will be made during GDA step 3 and step 4 to eliminate those gaps and to demonstrate that the risk is reduced to ALARP.

19.10 References

[1] ONR, Safety Assessment Principles for Nuclear Facilities, SAP, 2014.

[2] IAEA, Safety Requirements: Safety of Nuclear Power Plants: Design, No.SSR-2/1, Rev. 01, 2016.

[3] CGN, General Principles for Application of Laws, Regulations, Codes and

Standards, GHX00100018DOZJ03GN, Rev. F, 2018.

[4] WENRA, Safety Reference Levels for Existing Reactors, September 2014.

[5] WENRA, Safety of New Nuclear Power Plant Design, March 2013.

[6] IAEA, Safety Guide: Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.7, 2004.

[7] AFCEN, EPR Technical Code for Fire Protection, ETC-F, 2010.

[8] Health and Safety Executive, The Dangerous Substances and Explosive Atmospheres Regulations, 2002 No.2776, 2002.

[9] IAEA, Safety Guide: Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, NS-G-1.11, 2004.

[10] NRC, Standard Review Plan, NUREG 0800, 2007.

[11] IAEA, Safety Guide: Design of Fuel Handling and Storage Systems for Nuclear Power Plants, NS-G-1.4, 2003.

[12] NRC, Control of Heavy Loads at Nuclear Power Plants, NUREG 0612, 1980.

[13] NRC, Protection against Turbine Missiles, RG1.115, 2012.

[14] Health and Safety Executive, The Control of Major Accident Hazards Regulations, 2015 No. 483, 2015.

[15] American Concrete Institute, Code Requirements for Nuclear Safety Related Concrete Structures and Commentary, ACI 349-13, 2014.

[16] CGN, The General Requirements of Protection Design against Internal and External Hazards, GHX00100028DOZJ03GN, Rev. C, March 2018.

[17] GNS/CGN, Scope for UK HPR1000 GDA Project, HPR/GDA/REPO/0007, Rev.000.

[18] CGN, Internal and External Hazards Schedule Methodology Report, GHX00100044DOZJ03GN, Rev. C, April 2018.

[19] CGN, The Identification and Screening Process of Internal and External Hazards, GHX00100037DOZJ03GN, Rev. C, March 2018.

[20] BSI, BS EN 13501: Fire Classification of Construction Products and Building Elements, 2007.

[21] CGN, Fire Analysis Methodology Report, GHX00100022DOZJ03GN, Rev. B, March 2018.

[22] CGN, Methodology of Safety Categorisation and Classification,

GHX00100062DOZJ03GN, Rev. B, June 2018.

[23] BSI, BS476 Part 20:1987 - Fire Tests on Building Materials and Structures-Part 20: Method for Determination of the Fire Resistance of Elements of Construction (General Principles).

[24] CGN, Internal Explosion Safety Evaluation Methodology Report, GHX00100033DOZJ03GN, Rev. C, May 2018.

[25] CGN, External Explosion Safety Evaluation Methodology, GHX00100031DOZJ03GN, Rev. C, May 2018.

[26] CGN, Internal Flooding Analysis Methodology Report, GHX84200002DOZJ03GN, Rev. C, May 2018.

[27] CGN, High Energy Pipe Failures Safety Evaluation Methodology Report, GHX00100040DOZJ03GN, Rev. D, May 2018.

[28] ONR, Nuclear Safety Technical Assessment Guide for Internal Hazards, NS-TAST-GD-014, Rev. 4, 2016.

[29] CGN, Earthquake Safety Evaluation Methodology Report, GHX00100053DOZJ03GN, Rev. B, May 2018.

[30] CGN, Dropped Loads Safety Evaluation Methodology Report, GHX00100035DOZJ03GN, Rev. D, June 2018.

[31] CGN, Internal Missiles Safety Evaluation Methodology Report, GHX00100041DOZJ03GN, Rev. C, June 2018.

[32] CGN, Chemical Inventory for UK HPR1000, GHX00100012DOHB03GN, Rev. A, June 2018.

[33] CGN, ALARP Methodology, GHX00100051DOZJ03GN, Rev. B, April 2018.