Revision	Approved by	Number of Pages
000		103
Approval Date	12/11 2018	

General Nuclear System

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	HPR/GDA/PCSR/0014

Title:

Pre-Construction Safety Report

Chapter 14

Probabilistic Safety Assessment

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).

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

14.1 List of Abbreviations and Acronyms

ACPR1000	Advanced Chinese Pressurised Reactor
ALARP	As Low As Reasonably Practicable
AOS	Abnormal Operating State
ASEP	Accident Sequence Evaluation Program
ASG	Emergency Feedwater System (ASG [EFWS])
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BOP	Balance of Plant
BSL	Basic Safety Level
BSO	Basic Safety Objective
CAE	Claims, Arguments, Evidence
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failure
CD	Core Damage
CDF	Core Damage Frequency
CET	Containment Event Tree
CI	Conventional Island
DBC	Design Basic Condition
DCH	Direct Containment Heating
DEC-A	Design Extension Condition A
DEC-B	Design Extension Condition B
EHR	Containment Heat Removal System (EHR [CHRS])
FD	Fuel Damage
FDF	Fuel Damage Frequency
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
FV	Fussell-Vesely

GDA	Generic Design Assessment
GNS	General Nuclear System Limited
HBSC	Human-Based Safety Claim (HBSC)
HCLPF	High Confidence of Low Probability of Failure
HECP	Human Error Conditional Probability
HEP	Human Error Probability
HF	Human Factors (HF)
HFE	Human Failure Event
HPR1000	Hua-long Pressurised Reactor
HPR1000 (FCG3)	Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IB-LOCA	Intermediate Break (Loss of Coolant Accident)
I&C	Instrumentation and Control
IE	Initiating Event
ISLOCA	Interfacing Systems Loss of Coolant Accident
LB-LOCA	Large Break (Loss of Coolant Accident)
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPSD	Low Power and Shutdown
LRF	Large Release Frequency
MCCI	Molten Core-Concrete Interaction
MSIV	Main Steam Isolation Valve
MSQA	Management of Safety and Quality Assurance
NI	Nuclear Island
NPP	Nuclear Power Plant

NS/SG	Normal Shutdown with Steam Generators
NUREG	Nuclear Regulatory Commission technical report designation (US)
ONR	Office for Nuclear Regulation (UK)
PCSR	Pre-Construction Safety Report
PDS	Plant Damage State
PGA	Peak Ground Acceleration
PIE	Postulated Initiating Event
PMC	Fuel Handling and Storage System (PMC [FHSS])
POS	Plant Operating State
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factors
PTR	Fuel Pool Cooling and Treatment System (PTR [FPCTS])
PWR	Pressurised Water Reactor
PZR	Pressuriser
RBS	Emergency Boration System (RBS [EBS])
RC	Release Category
RCP	Reactor Coolant System (RCP [RCS])
RDF	Risk Decrease Factor
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RIF	Risk Increase Factor
RIS	Safety Injection System (RIS [SIS])
RPS	Reactor Protection System (RPS)
RPV	Reactor Pressure Vessel
RQ	Regulatory Query
RRI	Component Cooling Water System (RRI [CCWS])
SAP	Safety Assessment Principle (UK)

SAS	Safety Automation System
SB-LOCA	Small Break (Loss of Coolant Accident)
SEC	Essential Service Water System (SEC [ESWS])
SEL	Seismic Equipment List
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide (UK)
TEP	Coolant Storage and Treatment System (TEP [CSTS])
TEU	Liquid Waste Treatment System (TEU [LWTS])
UK HPR1000	UK Version of the Hua-long Pressurised Reactor
VDA	Atmospheric Steam Dump System (VDA [ASDS])
VVP	Main Steam System (VVP [MSS])

System codes (XXX) and system abbreviations (YYY) are provided for completeness in the format (XXX [YYY]), e.g. Extra Cooling System (ECS [ECS]).

14.2 Introduction

The Generic Design Assessment (GDA) for the UK Version of the Hua-long Pressurised Reactor (UK HPR1000) Pre-Construction Safety Report (PCSR) Chapter 14 presents Probabilistic Safety Assessment (PSA) work based on the UK HPR1000 design as described in Reference [1].

During the UK HPR1000 design process, PSA is used to demonstrate that a balanced design for the UK HPR1000 has been achieved, so that no particular feature or Postulated Initiating Event (PIE) makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent. The PSA is used to assure that small deviations in plant parameters, that could give rise to large variations in plant conditions (cliff edge effects), are prevented; and compares the results of the analysis with the radiation protection targets for risks that have been specified.

The UK HPR1000 PSA covers:

a) All sources of radioactivity at the facility, including the reactor core, Spent Fuel

Pool (SFP), radioactive wastes and new fuel.

1) Level 1 and Level 2 PSA for the reactor core are presented in Sub-chapter 14.4 and 14.5.

2) Level 1 and Level 2 SFP PSA are presented in Sub-chapter 14.6.The sources of radioactivity in SFP PSA include the SFP and fuel handing facilities in the Nuclear Island (NI).

3) Additional sources of radioactivity risk assessment are presented in Sub-chapter 14.7.

4) Level 3 PSA for all sources of radioactivity is presented in Sub-chapter 14.8.

b) All types of Initiating Events (IEs) (including internal events, internal hazards and external hazards).

1) Internal events for the reactor core are presented in Sub-chapter 14.4.1. Internal hazards and external hazards for the reactor core are presented in Sub-chapter 14.4.2.

2) Internal events for the SFP are presented in Sub-chapter 14.6.5. Internal hazards and external hazards for the SFP are presented in Sub-chapter 14.6.6.

3) Internal events, internal hazards and external hazards for additional sources of radioactivity are presented in Sub-chapter 14.7.

c) All plant operating states (POSs) for the reactor core and SFP.

1) Operating states for the reactor core are presented in Sub-chapter 14.4.1.5.

2) Operating states for the SFP are presented in Sub-chapter 14.6.5.1.

d) And Level 1, Level 2 and Level 3 PSA.

1) Level 1 PSA for the reactor core is presented in Sub-chapter 14.4. Level 1 for the SFP PSA is presented in Sub-chapters 14.6.5 and 14.6.6.

2) Level 2 PSA for the reactor core is presented in Sub-chapter 14.5. SFP Level 2 PSA is presented in Sub-chapter 14.6.7.

3) Level 3 PSA for all sources of radioactivity is presented in Sub-chapter 14.8.

14.2.1 Chapter Route Map

In-line with the Safety Case Route Map described in PCSR Chapter 1 taken in the development of UK safety cases, the UK HPR1000 PCSR follows a Claims, Arguments, Evidence (CAE) structure. Chapter 14 supports ***Claim 3.2*** and ***Claim 3.4***, derived from high-level, ***Claim 3*** which are described as follows:

Claim 3: *Nuclear safety: 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 (ALARP).

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

Claim 3.4: *The safety assessment shows that the nuclear safety risks are ALARP.*

To support the ***Claim 3.2 and Claim 3.4***, this chapter develops three Sub-claims, as follows:

a) ***Sub-Claim 3.2.4:*** *Probabilistic Safety Assessment is carried out to inform the design process and evaluate risk levels.*

b) ***Sub-Claim 3.4.6:*** *Probabilistic Safety Assessment demonstrates that the assessed risk levels meet the UK legal requirements and is ALARP.*

c) ***Sub-Claim 3.4.8:*** *All reasonably practicable options to improve nuclear safety have been adopted, demonstrating the risk is ALARP*

In order to support the three Sub-claims, Chapter 14 PSA develops a number of relevant arguments and evidences. The Argument 1 to Argument 5 and their evidences support the Sub-Claim 3.2.4. The Argument 1 to Argument 6 and their evidences support the Sub-Claim 3.4.6. The Argument 7 and its evidence support the Sub-Claim 3.4.8.

a) ***Argument 1:*** *The Methodology used for the UK HPR1000 PSA is acknowledged international good practice.*

  Evidence*: UK HPR1000 PSA methodology refers to the codes and standards listed in Sub-chapter 14.3. These defined the baseline requirements in codes and standards are well acknowledged good practice, and reflect international good practice. The methodology reports are as follows:*

  - *Methodology of Internal Event Level 1 PSA, Reference [2].*
  - *Methodology of PIE Identification, Reference [3].*
  - *Methodology of Human Reliability Analysis (HRA), Reference [4].*
  - *Methodology of Internal Fire PSA, Reference [5].*
  - *Methodology of Internal Flooding PSA, Reference [6].*
  - *Methodology of External Hazards PSA, Reference [7].*
  - *Methodology of Level 2 PSA, Reference [8].*
  - *Methodology of Spent Fuel Pool PSA, Reference [9].*

b) ***Argument 2:*** *The PSA covers all significant sources of radioactivity, all permitted operating states and all postulated initiating events.*

1) ***Evidence 1****: All significant sources of radioactivity are presented in PCSR Sub- chapters 14.2, 14.4, 14.6 and 14.7.*

2) ***Evidence 2****: All permitted operating states are mentioned in Sub-chapter14.4.1.5 and 14.6.5.1., described in Internal Events Level 1 PSA report and Internal Events SFP PSA report.*

3) ***Evidence 3****: All postulated initiating events are mentioned in Sub-chapter 14.4.1.6, 14.4.2.1, 14.6.5.2 and 14.6.6, and described in References [10], [11].*

c) ***Argument 3:*** *Data used in UK HPR1000 PSA are appropriate.*

Evidence: *Data used in the UK HPR1000 PSA reflect the latest information in nuclear industry.*

- *Data Analysis Report, Reference [12].*
- *Initiating Events Frequency is listed in Sub-chapter14.4.1.6 and Reference [10].*
- *Human Error Probability (HEP) will be listed in PSA reports.*

d) ***Argument 4:*** *The PSA adequately models the risk associated with the UK HPR1000, accounting for uncertainties and assumptions.*

Evidence: *The main assumptions for PSA models are listed in Sub-chapters 14.4.1.3, 14.4.2.1.1, 14.4.2.2.3, 14.4.2.3.3, 14.5.3, 14.6.3. The detailed assumptions and uncertainty analysis will be provided in PSA reports and models.*

e) ***Argument 5****: The PSA is used to support the development of design.*

1) ***Evidence 1:*** *The PSA has been used in the development process of HPR1000 design, and is described in Sub-chapter 14.10.1.1.*

2) ***Evidence 2****: The PSA is used to support UK HPR1000 design in GDA phase, and is described in Sub-chapter 14.10.1.2.*

f) ***Argument 6:*** *The PSA is used to evaluate related radiation protection targets and is ALARP.*

1) ***Evidence 1:*** *Related radiation protection targets will be described in Sub-chapter 14.9.*

2) ***Evidence 2:*** *The justification that process of PSA is ALARP is described in Sub-chapter14.10.2.1.*

g) ***Argument 7:*** *The PSA is used to inform the design to demonstrate ALARP.*

Evidence: *It is mentioned in Sub-chapter 14.10 that the PSA will be used to demonstrate that UK HPR1000 design is ALARP, and it will be further described in ALARP Demonstration for PSA report.*

14.2.2 Chapter Structure

Chapter 14 describes the PSA used in development of the UK HPR1000, and demonstrates that the UK HPR1000 will meet the requirements of UK context and the risk is reduced to be ALARP. The structure of Chapter 14 (Sub-chapter 14.4~ Sub-chapter 14.8) is based on the PSA steps undertaken, including Level 1, Level 2 and Level 3 PSA with the consideration of all radioactive sources. Radiation protection targets 5~9 evaluations and ALARP assessment are presented in Sub-chapter 14.9 and Sub-chapter 14.10.

The structure is as follows:

a) Sub-chapter 14.1 lists the specific abbreviations and acronyms within the PCSR Chapter 14.

b) Sub-chapter 14.2 presents the objective, route map, scope of this chapter, and interfaces with other chapters.

c) Sub-chapter 14.3 outlines the applicable codes and standards which are used for establishing the UK HPR1000 PSA.

d) Sub-chapter 14.4 presents the scope, approach, assumptions and the technical elements of the Level 1 PSA for the reactor core.

e) Sub-chapter 14.5 describes the scope, approach, assumptions and the technical elements of the Level 2 PSA for reactor core.

f) Sub-chapter 14.6 outlines the scope, approach, assumptions and the technical elements of the SFP PSA, including Level 1 and Level 2 SFP PSA.

g) Sub-chapter 14.7 outlines the scope, approach, assumptions of the risk assessment for additional sources of radioactivity.

h) Sub-chapter 14.8 describes the scope, approach and technical elements of the Level 3 PSA for all sources of radioactivity.

i) Sub-chapter 14.9 describes the scope and approach of the associated radiation protection targets evaluation.

j) Sub-chapter 14.10 presents the key insights and ALARP assessment for UK HPR1000 PSA to provide feedback on the risk level and influence improvements to plant design.

k) Sub-chapter 14.11 provides the summary of Chapter 14.

l) Sub-chapter 14.12 lists all references which are used for UK HPR1000 PCSR Chapter 14.

14.2.3 Interfaces with Other Chapters

PSA models and reports reflect and provide support to the associated chapters listed in T-14.2-1.

T-14.2-1 Interfaces between Chapter 14 and Other Chapters

PCSR Chapter	Interface
Chapter 1 Introduction	Chapter 1 provides the overall objectives, design reference and safety case route map for Chapter 14 PSA.
Chapter 3 Generic Site Characteristics	Chapter 3 provides generic site data for the hazards PSA in Chapter 14.
Chapter 4 General Safety and Design Principles	Chapter 14 provides the methodology and results of PSA which are based on the safety analysis principles set out in Chapter 4.
Chapter 6 Reactor Coolant System	Chapter 6 provides Reactor Coolant System (RCP [RCS]) design inputs for the PSA system analysis and fault tree modelling. Chapter 14 PSA is used to evaluate system reliability and support RCP [RCS] system design.
Chapter 7 Safety System	Chapter 7 provides design inputs for the PSA system analysis and fault tree modelling, including containment and related safety systems, the Safety Injection System (RIS [SIS]), Emergency Boration System (RBS [EBS]), and Atmospheric Steam Dump System (VDA [ASDS]) etc. Chapter 14 PSA is used to support safety system design and evaluate safety system reliability.
Chapter 8 Instrumentation and Control	Chapter 8 provides design inputs from the Reactor Protection System (RPS) and Safety Automation System (SAS) for the PSA system analysis and fault tree modelling.

PCSR Chapter	Interface
	The Chapter 14 PSA is used to support the system design of the RPS and evaluate safety system reliability.
Chapter 9 Electric Power	Chapter 9 provides the design inputs from off-site electrical power systems and on-site electrical power systems (including alternating current, direct current, emergency diesel generators and station black out diesel generators) for the PSA system analysis and fault tree modelling. Chapter 14 PSA is used to support electric power system design and evaluate the system reliability.
Chapter 10 Auxiliary System	Chapter 10 provides the design inputs from the auxiliary system (including Fuel Pool Cooling and Treatment System (PTR [FPCTS]), Component Cooling Water System (RRI [CCWS]) and Essential Service Water System (SEC [ESWS])) for the PSA system analysis and fault tree modelling. Chapter 14 PSA is used to support the design of the auxiliary system and evaluate the system reliability.
Chapter 11 Steam and Power Conversion System	Chapter 11 provides the steam and power conversion system design inputs (including Main Steam System (VVP [MSS]), Main Feedwater Flow Control System (ARE [MFFCS]), etc.) for the PSA system analysis and fault tree modelling. Chapter 14 PSA is used to support the system design and evaluate the system reliability.
Chapter 12 Design Basis Condition Analysis	Chapter 12 provides a PIE list for determining the PSA IE list. Chapter 14 PSA provides IE frequencies for supporting the definition of Design Basic Conditions (DBC).

PCSR Chapter	Interface
Chapter 13 Design Extension Conditions and Severe Accident Analysis	Chapter 13 provides safety case calculations as an input to the Level 1 and Level 2 PSA, including contributions to containment breach frequency. Chapter 14 provides accident sequences to support source term calculation and the PSA provides the accident sequences for identifying Design Extension Condition A (DEC-A) and Design Extension Condition B (DEC-B).
Chapter 15 Human Factors	Chapter 15 provides the scope, methodology and principle of HRA in PSA. It also substantiates the claims on operator actions to support an iterative analysis of PSA. Chapter 14 PSA provides the significant analysis results for Human Error Events (HEE) to support task analysis in Human Factors.
Chapter 16 Civil Works & Structures	Chapter 16 provides internal containment performance evaluation for Level 2 PSA. Chapter 14 describes the methodology of internal containment performance evaluation.
Chapter 18 External Hazards	Chapter 18 provides the design basis and protection measures information of external hazards to Chapter 14. Chapter 14 evaluates the risk of external hazards and provides risk insights to support the design of external hazards.
Chapter 19 Internal Hazards	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.

PCSR Chapter	Interface
Chapter 20 Management of Safety and Quality Assurance (MSQA) & Safety Case Management	The organisational arrangements and quality assurance arrangements set out in Chapter 20 are implemented in the design process and production of Chapter 14.
Chapter 23 Radioactive Waste Management	Chapter 23 provides the radioactive waste design basis and related system design to support for sources of radioactivity risk PSA. The Chapter 14 PSA is used to support the system design of related radioactive waste management and evaluate safety system reliability.
Chapter 28 Fuel Route and Storage	Chapter 28 provides the layout and process of Fuel Handling and Storage System (PMC [FHSS]), which is a design input for the SFP PSA. Chapter 14 provides the main results of the PSA and risk insights for the PMC [FHSS].
Chapter 33 ALARP Assessment	Chapter 14 provides the analysis of risk and the evaluation of radiation protection targets for fault and accident condition which supports the overall ALARP demonstration addressed in Chapter 33.

14.3 Applicable Codes and Standards

The UK HPR1000 PSA is developed in accordance with international practices and requirements of UK context. The applicable codes and standards which are used for developing UK HPR1000 PSA are selected according to General Principle for Applications of Laws, Regulations, Codes and Standards, Reference [15].

The selection principles of applicable codes and standards for the UK HPR1000 PSA are as follows.

a) The Relevant Good Practices (RGPs) of international organisations (e.g. IAEA, WENRA) or other countries (e.g. UK, US and France), are taken into account as appropriate.

b) The relevant experience provided in guidance documents, design codes and standards used for other GDA projects is taken in to account.

c) Latest versions of guidance documents, design codes and standards are preferred to ensure latest good practices are captured.

Based on the principles, codes and standards adopted for the development of the UK HPR1000 PSA are listed in T-14.3-1.

T-14.3-1 Codes and Standards Supporting the Development of the UK HPR1000 PSA

Standard No.	Title	Date Issued	Applied PSA Scope	Project Used
SSG-3	Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants	2010	Internal event Level 1 PSA, Hazards PSA	UK ABWR, HPR1000 (FCG3)
SSG-4	Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants	2010	Level 2 PSA	UK ABWR, HPR1000 (FCG3)
IAEA-TECDOC-1804	Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants.	2016	Internal event Level 1 PSA, Hazards PSA	---
ASME/ANS RA-Sb-2013	Addenda to ASME/ANS RA-S 2008: Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications	2013	Level 1 PSA	UK ABWR, HPR1000 (FCG3)
ASME/ANS RA-S-1.2-2014	Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs)	2014	Level 2 PSA	---

Standard No.	Title	Date Issued	Applied PSA Scope	Project Used
ASME/ANS RA-S-1.3-2017	Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications	2017	Level 3 PSA	---
NUREG/CR-6850	Fire PRA Methodology for Nuclear Power Facilities	2005	Internal fire PSA	UK EPR, UK AP1000, UK ABWR, HPR1000 (FCG3)
NUREG/CR-4772	Accident Sequence Evaluation Program Human Reliability Analysis Procedure	1987	Human reliability analysis	UK EPR, HPR1000 (FCG3)
NUREG/CR-6883	The Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) Method	2005	Human reliability analysis	UK EPR, UK ABWR, HPR1000 (FCG3)
EPRI TR-3002000709	Seismic Probabilistic Risk Assessment Implementation Guide	2013	Seismic PSA	UK ABWR, HPR1000 (FCG3)
EPRI NP-6041-SLR1	A Methodology for Assessment of Nuclear	1991	Seismic PSA	HPR1000 (FCG3)

Standard No.	Title	Date Issued	Applied PSA Scope	Project Used
	Power Plant Seismic Margin (Revision 1)			
EPRI TR-103959	Methodology for Developing Seismic Fragilities	1994	Seismic PSA	UK EPR, HPR1000 (FCG3)
EPRI-1019194	Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment	2009	Internal flooding PSA	UK AP1000, HPR1000 (FCG3)
EPRI 1019259	Fire Probabilistic Risk Assessment Methods Enhancements	2010	Internal fire PSA	HPR1000 (FCG3)

14.4 Level 1 PSA

The Level 1 PSA in this sub-chapter is focussed on the reactor core only. The scope includes all plant operating states (full power, Low Power and Shutdown (LPSD)), and all IEs (including internal events, internal and external hazards). The Level 1 PSA for the spent fuel pool is presented in Sub-chapters 14.6.5 and 14.6.6.

The Level 1 PSA methodology for UK HPR1000 follows the codes and standards presented in References [16], [17] and [18]. These codes and standards are well acknowledged good practice, and reflect the latest progress and most mature practice. The methodology reports are listed in References [2], [3], [4], [5], [6] and [7].

For the Level 1 PSA, the current UK HPR1000 design is analysed in order to identify the sequences of events that can lead to core damage. Core Damage Frequency (CDF) is analysed as part of the Level 1 PSA.

PIE is defined as an event identified during design capable of leading to anticipated operational occurrences or accident conditions, including internal events as described in Reference [3]. A Level 1 PSA IE for the reactor core is a PIE that could lead directly to core damage (e.g. reactor vessel rupture) or that challenges normal operation, which requires successful mitigation using safety or non-safety systems to prevent core damage, as described in Reference [16]. IEs in Level 1 PSA include internal events (in Sub-chapter 14.4.1), internal and external hazards (in Sub-chapter 14.4.2).

For the Level 1 PSA, event trees are used for estimating CDF due to each IE. Fault trees are used for estimating the failure probability of the systems or components. The risk quantification and event tree/fault tree modelling have been carried out using the Risk Spectrum professional software (version 1.2.1). This enables the integration of the fault tree models with the event tree models.

14.4.1 Internal Events Level 1 PSA

14.4.1.1 Introduction

The internal events Level 1 PSA is performed during the UK HPR1000 design process to support and optimise the design of systems and processes. This enables the achievement of a well-balanced system and process design.

This sub-chapter covers the scope, main assumptions, methodology and technical elements for the internal events Level 1 PSA.

14.4.1.2 Scope

The internal events Level 1 PSA is predominantly focussed on the consideration of internal IEs that can cause core damage, or are mitigated to prevent core damage. It covers all plant operating states (full power and LPSD states).

14.4.1.3 Assumptions

For the internal events Level 1 PSA, the main assumptions are listed as follows:

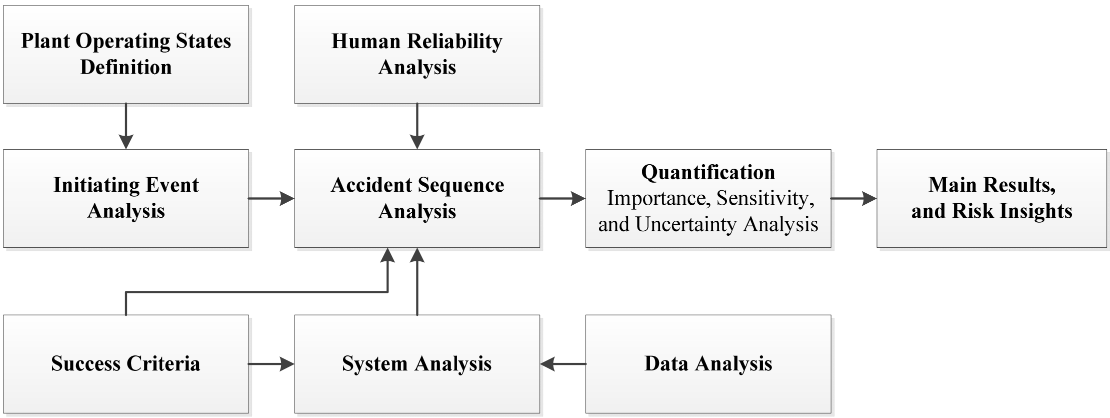
a) In fault tree modelling, only two states (i.e. success or failure) are considered for the top event and every basic event.

b) In fault tree modelling, a component may be excluded from the system model if the total failure probability of the component failure resulting in the same effect on system operation is at least two orders of magnitude lower than the highest failure probability of other components in the same system that result in the same effect on system operation, Reference [17].

c) Mission time is assumed to be 24 hours. For many initiating events, this period of time is sufficient for the reactor to reach a safe state and for long term measures to be put in place to maintain this state. Mission times with other values are discussed on a case-by-case basis.

14.4.1.4 Methodology

The internal events Level 1 PSA for the UK HPR1000 follows the requirements presented in References [16], [17] and [18]. The methodology of the internal events Level 1 PSA can be summarised as figure F-14.4-1.



F-14.4-1 Flow Chart of the Internal Events Level 1 PSA

The main technical elements adopted for the internal events Level 1 PSA are as follows.

a) Plant operating states.

b) IEs analysis.

c) Accident sequence analysis.

d) Success criteria.

e) System analysis.

f) Human reliability analysis.

g) Data analysis.

h) Quantification.

The detailed analysis methodology for the above technical elements in the UK HPR1000 PSA is provided in Reference [2].

14.4.1.5 Plant Operating States

For the internal events Level 1 PSA, all standard operating conditions are considered from POS A to POS G defined in T-14.4-1. In order to ensure each standard operating condition can be analysed appropriately, the states are grouped using a qualitative assessment. The general approach to grouping is primarily based on:

a) Similarity of plant status;

b) Similarity of available systems and components;

c) Similarity of potential IEs.

For the UK HPR1000 internal events Level 1 PSA, the POSs are defined according to Reference [19]. The POSs for the UK HPR1000 PSA are listed in the following table.

T-14.4-1 Definition of Plant Operating States

POS	**Standard Operating Conditions**	**RCP [RCS] State**	**Coolant Inventory**	**RCP [RCS] Average Temperature (°C)**	**RCP [RCS] Pressure (bar abs)**
POS A	Reactor in power	closed	Pressuriser (PZR)level is at set point	295≤T≤307	155
	Hot standby	closed	PZR level is at set point	295	155
	Hot shutdown	closed	PZR level is at set point	295	155
	Intermediate shutdown with NS/SG connection conditions (P≥130 bars abs)	closed	PZR level is at set point	T<295	130≤P<155
POS B	Intermediate shutdown with NS/SG connection conditions (P<130 bars abs)	closed	PZR level is at set point	[T＞135 and 32≤P<130]; [T＞140 and P≤32]	

<table>
<tr><th>POS</th><th>Standard Operating Conditions</th><th>RCP [RCS] State</th><th>Coolant Inventory</th><th>RCP [RCS] Average Temperature (°C)</th><th>RCP [RCS] Pressure (bar abs)</th></tr>
<tr><td></td><td>Intermediate shutdown with RIS-RHR connection conditions</td><td>closed</td><td>PZR level is at set point</td><td>135≤T≤140</td><td>24≤P≤32</td></tr>
<tr><td rowspan="4">POS C (POS G*)</td><td rowspan="3">Intermediate shutdown with RIS-RHR</td><td>closed</td><td rowspan="3">PZR level is at set point or full</td><td>100≤T≤140</td><td>24≤P≤32</td></tr>
<tr><td>closed</td><td>10≤T<100</td><td>24≤P≤32</td></tr>
<tr><td>closed</td><td>10≤T≤60</td><td>P≤32</td></tr>
<tr><td>Normal cold shutdown (RCP [RCS] pressurisable)</td><td>Non-closed and pressurisable</td><td>≥¾ loop level</td><td>10≤T≤60</td><td>P≤32</td></tr>
<tr><td rowspan="2">POS D (POS G*)</td><td rowspan="2">Normal cold shutdown for maintenance (RCP [RCS] not pressurisable)</td><td>Non-closed and not pressurisable, Reactor cavity non fillable</td><td rowspan="2">≥¾ loop level</td><td rowspan="2">10≤T≤60</td><td rowspan="2">Atmospheric pressure</td></tr>
<tr><td rowspan="2">Non-closed and not pressurisable Reactor cavity fillable</td></tr>
<tr><td>POS E</td><td>Normal cold shutdown for refuelling</td><td>Reactor cavity flooded</td><td>10≤T≤60</td><td>Atmospheric pressure</td></tr>
<tr><td>POS F</td><td>Core totally unloaded</td><td>---</td><td>---</td><td>---</td><td>---</td></tr>
</table>

*Where POS G is a particular plant operating state during POS C and POS D, in which the reactor coolant inventory is near the mid-loop water level. This brings additional risk and shall be considered separately.

14.4.1.6 Initiating Events Analysis

The IEs considered in this sub-chapter are internal events mainly caused by random component failure or human errors.

The objectives of the IE analysis are to identify and quantify IEs. IE analysis is performed according to the following four steps (as Reference [3]):

a) Identifies a reasonably complete IEs list.

b) Groups the IEs according to similar mitigation requirements to facilitate modelling but realistic estimation of CDF.

c) Provides a completeness analysis of the IEs list through comparison with existing IE lists and evaluates this against operating experience feedback.

d) Estimates the IE frequencies for the group.

14.4.1.6.1 Initiating Events Identification

Master logic diagram and Failure Mode and Effect Analysis (FMEA) are used to identify PIEs for the UK HPR1000, Reference [3].

a) Master Logic Diagram Analysis

The master logic diagram analysis begins with radioactive material release, then step by step looks for the direct causes associated (regardless of the successful operation of the preventative measures), and identifies all possible Abnormal Operating States (AOSs) . The basic events that can possibly lead to AOSs are considered as potential postulated IEs.

b) Failure Mode and Effect Analysis

It is considered as a complementary analysis to ensure the completeness of postulated IEs identified from the master logic diagram analysis. Results are combined to form a comprehensive list.

The detailed methodology of initiating event identification, used as part of the deterministic safety analysis and PSA, is presented in Reference [3].

14.4.1.6.2 Initiating Events Grouping

In order to limit the analysis required for the Level 1 PSA to a manageable size, a grouping process needs to be carried out before proceeding to the accident sequence analysis.

The postulated IEs identified for the UK HPR1000 design can be grouped according to the similarity in plant response, success criteria, timing, and the effect on the operability and performance of operators and relevant mitigating systems. Postulated IEs can be subsumed into a group and bounded by the worst case impacts within the group.

However, initiating event categories with different plant response impacts (i.e. those with different success rate criteria) or those with a more severe radionuclide release potential should be grouped separately from other IE categories. This could include initiators such as Reactor Pressure Vessel (RPV) rupture, loss of coolant accident with containment bypass, steam generator tube ruptures (SGTR), and non-isolated breaks outside containment.

14.4.1.6.3 IE List Completeness Analysis

Evaluating the completeness of the IE list for the UK HPR1000 PSA includes operating experience feedback and comparison against existing PSA IE lists.

Existing IE lists are attained from similar Pressurised Water Reactor (PWR) Nuclear Power Plants (NPP) around the world.

14.4.1.6.4 Initiating Events Frequency Estimation

Frequencies of IEs (group) are derived from one of the following sources:

a) Data from generic site reports, Reference [24], such as the frequency of Loss of Offsite Power (LOOP).

b) Data from NUREG series, such as breaks of primary system and secondary system.

c) The operating experiences data of similar plants, such as maintenance LOCA, transients, cold overpressure and homogeneous boron dilution accidents.

d) Data from Fault Tree Analysis (FTA), such as loss of cooling chain and loss of Residual Heat Removal (RHR).

However, an IE whose frequency or risk is very low will be eliminated from further evaluation in this step.

According to the above methodology, the IEs (group) list used in the Level 1 PSA is presented in Reference [10] and listed in T-14.4-2.

T-14.4-2 IEs List of Internal Events

No.	IE Description	POS	Frequency (Per Reactor Year)
1.	Large Break (Loss of Coolant Accident)	POS A	{ }
		POS B	{ }
2.	Intermediate Break (Loss of Coolant Accident)	POS A	{ }
		POS B	{ }
3.	Small Break (Loss of Coolant Accident)	POS A	{ }
		POS B	{ }
		POS C	{ }
		POS D	{ }

No.	IE Description	POS	Frequency (Per Reactor Year)
		POS G	{ }
4.	Stuck Open of Pressuriser Safety Valve	POS A	{ }
		POS B	{ }
5.	Isolable Maintenance Breaks (Loss of Coolant Accident)	POS C	{ }
		POS D	{ }
		POS G	{ }
6.	Non-isolable Maintenance Breaks (Loss of Coolant Accident)	POS C	{ }
		POS D	{ }
		POS G	{ }
7.	Interfacing Systems Loss of Coolant Accident	POS A	{ }
		POS B/ POS C/ POS D /POS G	{ }
8.	Reactor Pressure Vessel Rupture	POSA	{ }
9.	Loss of Offsite Power	POS A	{ }
		POS B	{ }
		POS C	{ }
		POS D	{ }
		POS G	{ }
10.	Steam Generator Tube Rupture （one tube）	POS A	{ }
		POS B	{ }
11.	Steam Generator Tube Rupture	POS A	{ }

No.	IE Description	POS	Frequency (Per Reactor Year)
	(two tubes)	POS B	{ }
12.	Main Steam Line Breaks inside Containment	POS A	{ }
		POS B	{ }
13.	Main Steam Line Breaks between Containment and Main Steam Isolation Valve (MSIV)	POS A	{ }
		POS B	{ }
14.	Main Steam Line Breaks Downstream of MSIV	POS A	{ }
		POS B	{ }
15.	Main Feedwater Line Breaks Between the Check Valve and SG	POS A	{ }
		POS B	{ }
16.	Main Feedwater Line Breaks Upstream of the Check Valve	POS A	{ }
		POS B	{ }
17.	Primary System Transients	POS A	{ }
18.	Secondary System Transients with RCP [RCS] Temperature Decrease	POS A	{ }
19.	Secondary System Transients with RCP [RCS] Temperature Increase	POS A	{ }
20.	Loss of Main Feedwater	POS A	{ }
21.	Cold Overpressure of the Primary System	POS C	{ }
22.	Total Loss of Cooling Chain	POS A	{ }
		POS B	{ }

No.	IE Description	POS	Frequency (Per Reactor Year)
		POS C	{ }
		POS D	{ }
		POS G	{ }
23.	Loss of Startup and Shutdown Feedwater System	POS B	{ }
24.	Loss of Vital Direct Current Power	POS A	{ }
25.	Loss of Vital 10kV Emergency Power Distribution System Bus	POS A	{ }
		POS B	{ }
26.	Loss of Residual Heat Removal (including the Loss of Vital 10kV Emergency Power Distribution System Bus)	POS C	{ }
		POS D	{ }
		POS G	{ }
27.	Homogeneous Boron Dilution	POS A	{ }
		POS B	{ }
		POS C	{ }
		POS D	{ }
		POS G	{ }

14.4.1.7 Accident Sequence Analysis

Accident sequences are described by event trees and start with an IE followed by success or failure of safety functions. There are two different kinds of accident sequence end states, one is core damage, and the other is successful accident mitigation. Accident sequence end states are core damage if the minimum required system functions are not performed.

An event tree graphically models the plant response for the mitigation of IEs through success or failure of events called function events. Function events of an event tree can be a status of safety function, the status of system, a basic event occurrence or an operator action.

The function events are normally arranged in either chronological or causal order. Chronological ordering means that events are considered in the order in which they are expected to occur in an accident. Causal ordering means that events are arranged in the event tree so that the number of omitted branch point is maximised. Chronological ordering is preferentially used.

Small event tree/large fault tree approach is used in UK HPR1000 PSA modelling. As a result, the event trees are concise and allow a synthesised view of accident sequences. The fault trees are discussed in ‘System Analysis’ (Sub-chapter 14.4.1.9).

In the UK HPR1000 internal events Level 1 PSA, accident sequences are modelled with two kinds of event tree, which are pre-trees and main event trees. Pre-trees are event trees where the initiating events are defined with their frequencies, and the associated accidents information, such as break size and location, reactor trip success or not, number of ruptured steam generator tubes, etc. Main event trees are event trees where the majority of accident mitigation functions (e.g. secondary side cooling functions with Emergency Feedwater System (ASG [EFWS]) and Atmospheric Steam Dump System (VDA [ASDS]), or medium or low head safety injection functions with RIS [SIS]) are modelled to develop the accident sequences. Pre-trees are connected to main event trees by the consequences defined in pre-trees, e.g. the SB-LOCA pre-tree is connected to the SB-LOCA event tree using the consequence “SLOCA_A” for the modelling of a small LOCA accident during POSA.

14.4.1.8 Success Criteria

Success criteria for the internal events Level 1 PSA are defined for systems that fulfil the following functions:

a) Reactivity control.

b) Heat removal from the reactor.

To meet the success criteria defined for the internal events Level 1 PSA model, the plant should be able to achieve and maintain a safe state for at least 24 hours, Reference [16]. Sequences that do not meet the relevant success criteria are assigned to a core damage end state.

For the UK HPR1000 internal events Level 1 PSA accident sequence analysis, end states are clearly defined to be Core Damage (CD) or successful mitigation (OK).

CD is defined as (in accordance with Reference [17]) uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated, involving enough of the core where, if released, it would result in offsite public health effects in the form of a radiation dose. The plant parameters (e.g., highest node temperature, core collapsed liquid level) and associated acceptance criteria have been used in determining whether core damage occurs or not. These parameters are selected such that the determination of core damage is as realistic as practicable, in a manner consistent with current best practice. The UK HPR1000 PSA, criterion used to determine CD is a peak cladding temperature higher than 982°C.

OK indicates that the system functions and human actions carried out in response to the IE have ensured that the core damage criteria are not exceeded.

If a significant time interval is required to result in core damage following exposure of the top of the core, this is taken into account when generating a realistic definition for core damage.

The success criteria are consistent with plant design. The success criteria for each safety system are defined as the minimum level of performance required to achieve the safety function, taking into account the specific features of each sequence. The success criteria also specify the mission time for the safety systems, that is, the time that the safety systems need to operate so that the reactor reaches a safe state and long term measures can be put in place to maintain this state. The success criteria define the operator actions required to bring the plant to a safe state as defined by the plant procedures.

14.4.1.9 System Analysis

System analysis is used to identify and quantify the causes of failure for each plant system presented in the IE and accident sequence analysis.

Systems which need to be considered in the system analysis can be divided into two categories:

a) Front-line systems: a system (safety or non-safety) that is capable of performing a direct accident mitigating function modelled in the PSA, such as the RIS [SIS] or ASG [EFWS].

b) Support systems: a system that support the accident mitigation function (electrical power, Instrumentation and Control (I&C), cooling, and Heating, Ventilation and Air Conditioning (HVAC), etc.).

The following contents are considered in the system analysis.

a) Configuration of systems before and after the start of their operation in an accident sequence is defined. System success criteria are stated, and necessary actions and claimed components are identified. Here, generation and transition of initiation signals for demanded components and operator actions are identified and modelled. All failure modes for demanded components are listed in the summary of the failure mode analysis, with consideration made to Common Cause Failure (CCF). Support systems for demanded components are also investigated and listed.

b) Factors degrading safety function such as flow bypass, flow blockage and spurious signals are identified and added to the summary of failure mode analysis.

c) Other factors leading to system unavailability conditions are investigated such as unavailability due to maintenance and human factors.

A fault tree analysis is used to model all system functions. The main contents of the FTA include:

a) Determination of the top event.

b) Construction of a fault tree.

c) Qualitative and quantitative analysis of fault tree.

For the system analysis, it is important to note that some components with the same design and manufacture, and working in the same environment may fail due to the same causes, resulting in a higher failure probability than would result from independent failure. So it is necessary to quantify CCF events in system fault trees.

The identification of common cause failures considers similarities between components, based on operation, environment design, maintenance and testing similarities.

A logical and systematic process is used to define CCF groups for UK HPR1000 systems, which considers similarities in service conditions, environment, design and manufacture, and maintenance. There are several kinds of components that are considered to be susceptible to common cause failure in the UK HPR1000 PSA model, such as electrical motor valves, check valves, pumps, diesel generators and sensors.

14.4.1.10 Human Reliability Analysis

HRA is an important element of PSA in order to gain an understanding of risks in the UK HPR1000 design. For UK HPR1000 PSA, Human Factors (HF), PSA and Fault Studies are be integrated to support HRA in PSA

The PSA analysis results will be provided to the human factors assessment as inputs for identifying the Human-Based Safety Claim (HBSC) that are described in Sub-chapter 15.7 and evaluating their importance to UK HPR1000 risk.

Furthermore, a detailed task analysis will be carried out to justify the results of HRA in PSA， and the PSA model will be updated depending on results of task analysis.

Human activities can mitigate potential consequences, but can also lead to accidents. The responses of different systems and human behaviours constitute different accident processes. The following three types of HFE are considered in PSA modelling, Reference [4]:

a) Pre-initiating events HFEs (Type A);

b) HFEs that lead to initiating events (Type B);

a) Post-initiating events HFEs (Type C).

14.4.1.10.1 Type A Human Failure Event Analysis

Type A HFEs occur as a result of routine maintenance, testing or calibration activities (before an IE) resulting in unavailability of the associated safety component. The analysis steps are as follows

a) Step 1: Systems Identification

The systems modelled in an internal event Level 1 PSA, Level 2 PSA, internal/external hazards PSA and SFP PSA predominantly consider the analysis of type A HFEs.

b) Step 2: Human Activities Identification

This step is to identify those specific routine human activities that, if not completed correctly, might impact the availability of equipment necessary to perform the system function modelled in the PSA.

c) Step 3: Equipment Identification

According to the system equipment and human activities identified, the equipment influenced by the human activities can be determined. If the state of equipment is changed during human activities, it is considered as equipment influenced by human activities.

d) Step 4: Equipment Screening

If equipment influenced by human activities meets one of the following criteria, it is screened out:

1) Equipment that is automatically reset/realigned and available when demanded.

2) Equipment for which the position and status can be routinely checked and realigned from the main control room based on real-time indications.

e) Step 5: HEP Calculation

For the UK HPR1000 PSA, the methodology of the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP) in Reference [20] is used to calculate the HEP of the type A HFEs.

14.4.1.10.2 Type B Human Failure Event Analysis

Type B HFEs are human errors which could lead to IEs. The frequency calculation of initiating events has two methodologies:

a) Using the generic data or experience data

For this type of IE, the frequency of IEs caused by HFEs has been based on existing generic data or operating experience. Therefore, for this type of IE, the HFEs are analysed as part of the HRA.

b) Using IE fault trees

The HFEs leading to this type of IE are analysed in detail. The analysis steps are as follows:

1) Step 1: IE Fault Trees Identification

This step is used to develop the IE fault trees and identify those functions where failure may lead to the occurrence of top events from the fault trees.

2) Step 2: Human Failure Events Identification

This step is used to identify the HFEs leading to functions where, following failure, lead to the occurrence of top events from the fault trees.

3) HEP Calculation

The HEP is calculated by using the database in Reference [21]. According to Reference [22], the lower bound cut-off value of 1.0E-5 for HEPs is used in the type B human failure events in the UK HPR1000 PSA.

14.4.1.10.3 Type C Human Failure Event Analysis

Type C HFEs occur when the operators diagnose accident responses after an accident and complete the corresponding operation. Type C HFEs involve the diagnosis and activity performed by operators. Therefore, it is different for each IE. Type C HFEs are predominantly considered as part of fault or event trees. The analysis steps are as follows:

a) Human Activities Identification

For the UK HPR1000 PSA, the accident sequence is analysed systematically; the operator response in each sequence is identified for each human activity.

b) Qualitative Analysis

HEP calculation is based on qualitative analysis. The purpose of qualitative analysis is to describe in detail the HFEs and their influence, and to determine the important influencing factors that should be considered in the modelling process. Human task description and analysis are carried out to divide a task into its constituent parts, to identify errors, violations and recovery opportunities; to calculate task duration and correctly interpret the quality of Performance Shaping Factors (PSFs) and crew response activities.

c) HEP Calculation

Type C HFEs for the UK HPR1000 are assessed using the SPAR-H approach, Reference [22]. The SPAR-H approach assesses human errors from two aspects: diagnosis errors and action errors. For diagnosis errors and action errors, the SPAR-H takes into account the impact of 8 PSFs respectively, and qualifies them as weighted values to reflect in the quantitative analysis process. These 8 PSFs are available time, stress/stressors, complexity, experience/training, procedures, ergonomics/Human Machine Interface (HMI), fitness for duty and work processes. PSFs are defined in Reference [4].

14.4.1.10.4 Dependency Analysis

In the HRA of the UK HPR1000 PSA, the dependencies between/among HFEs have been considered to avoid the potential to underestimate the risk. The potential impacts of dependency between/among separate activities are assessed using the following process.

a) Step 1: Dependencies Identification

In the HRA, the following dependencies between/among HFEs are identified:

1) Dependency between/among Type A HFEs.

2) Dependency between/among Type B HFEs.

3) Dependency between/among Type C HFEs.

4) Dependency between/among Type A HFEs and Type B HFEs.

5) Dependency between/among Type A HFEs and Type C HFEs.

6) Dependency between/among Type B HFEs and Type C HFEs.

7) Dependency between/among Type A HFEs, Type B HFEs and Type C HFEs.

b) Step 2: Assignment of Dependency Level

The following variables (crew, time, location, and cues) are considered to construct a dependency matrix. According to Reference [22], T-14.4-3 presents the dependency table that can be used to assign a dependency level to the UK HPR1000 PSA.

T-14.4-3 Dependency Rating System

Crew, Time, Location and Cue Assignments	Dependency Level
Same crew, close in time, same location, with or without additional cues	Complete
Same crew, close in time, different location, with or without additional cues	High
Same crew not close in time, same location, no additional cues	High
Same crew, not close in time, same location, additional cues	Moderate
Same crew, not close in time, different location, no additional cues	Moderate
Same crew, not close in time, different location, additional cues	Low
Different crew, close in time, same location, with or without additional cues	Moderate
Different crew, not close in time, same location, no additional cues	Low

c) Human Error Conditional Probability Calculation

The HEP is the probability of HFE without formal dependence, and the Human Error Conditional Probability (HECP) is the probability of an HFE with formal dependence. According to Reference [21], the calculation of HECP in the UK HPR1000 PSA is undertaken as follows:

1) For the level of complete dependence, the HECP of the last HFEs is 1.

2) For a high level of dependence, the HECP of the last HFEs is (1+ HEP)/2.

3) For a moderate level of dependence, the HECP of the last HFEs is (1+6×HEP)/7.

4) For a level of low dependence, the HECP of the last HFEs is (1+19×HEP)/20.

14.4.1.11 Data Analysis

Data analysis is used to provide the data used in the PSA model, including the IE frequency, reliability data and HEPs. The IE frequency is defined in Sub-chapter 14.4.1.6, and the HEP is defined in Sub-chapter 14.4.1.10. The reliability data for components is discussed in this sub-chapter.

In general, the component failures include failure on demand and failure during operation. The data are sorted by generic data and plant specific data. Generic data is such data that reflects the industry average performance of the nuclear power plant operation. Plant specific data means the data consisting of observed sample data from plant analysis, Reference [17]. Since plant specific data are not available in the GDA phase, predominantly, generic data are used with consideration of applicable operating data from similar plants when possible and appropriate.

The reliability data of component and CCF parameters for UK HPR1000 PSA are referred to Reference [12].

The principles of database selection are as follows:

a) The database needs to reflect the latest statistics of the nuclear industry;

b) The selection of database sources for different types of components should be as consistent as possible.

The hierarchy of data sources is listed below:

a) Chinese components reliability data report for nuclear power plants

The database reflects the latest operating experience for Chinese nuclear power plant, and has been combined with the generic data of Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (NUREG/CR-6928 (version 2007)) by Bayesian update. Therefore, it can reflect the current nuclear power plant component reliability level.

b) NUREG/CR-6928 (version 2015)

The data in Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (NUREG/CR-6928 (version 2015)), Reference [13] is from US operating experience, mostly covering 1998 to 2015. This database is taken as a supplement when no data was found in Chinese Components Reliability Data Report for Nuclear Power Plant.

c) CCF data

CCF refers to that some components with the same design and manufacture, and working in the same environment may fail due to the same causes. As a generic CCF parameters database in NUREG/CR-5497, Reference [14], which covers a large group of components is used for UK HPR1000.

14.4.1.12 Quantification

The quantification process for the internal events Level 1 PSA aims to provide an estimate of CDFs for the UK HPR1000 based on core damage scenarios including overall CDF and CDF following each applicable accident sequence. As part of the quantification process, the cut-off value is selected to be 1.0E-13, so probability values less than 1.0E-13 are not considered further, Reference [2]

During the PSA quantification process, one important task is the qualitative discussion and quantitative evaluation of uncertainties of the PSA analysis results. A major advantage of PSA is that it provides an explicit framework for the analysis of risk uncertainties. The identification of sources of uncertainty and an understanding of their implications in the PSA model and its results should be considered an inherent part of any PSA, so that, when the results of the PSA are used to support a decision, the impact of the uncertainties can be taken into account, Reference [16].

In a system fault tree or an accident sequence, different basic events are at different positions in the logic model and have different probabilities (frequencies) of occurrence; as a result, they have different contributions to risk. The degree of such contributions is called importance. Importance analysis of basic events aims to analyse the degree of such contributions of different basic events. The various importance measures provide a perspective on which basic events, etc., contribute most to the current estimate of risk (Fussell-Vesely (FV) importance, Risk Decrease Factor (RDF)), which contribute to maintaining the level of safety (Risk Increase Factor (RIF)), Reference [16].

A sensitivity analysis is carried out for the assumptions and data that have a significant level of uncertainty and which are likely to have a significant impact on the results of the Level 1 PSA. The sensitivity studies should be carried out by re-quantifying the analysis using alternative assumptions or by using a range of numerical values for the data that reflects the level of uncertainty, Reference [16].

14.4.1.13 Main Results and Risk Insights

This section will provide a summary of the internal events Level 1 PSA results. The results include:

a) Total CDF of internal events at full power state and LPSD states;

b) Contributions of core damage frequencies by various groups of internal event IEs;

c) Contributions by different POSs;

d) Dominant core damage sequences;

e) Minimal cut-set analysis results;

f) Importance analysis results;

g) Sensitivity analysis results;

h) Uncertainty analysis results;

i) Risk insights.

14.4.2 Internal and External Hazards Level 1 PSA

Hazards can be categorised into internal hazards and external hazards. According to Reference [11], the definitions are as follows:

Internal hazards are those hazards to the facility or its Structures, Systems and Components (SSC) that originate within the site boundary and over which the duty-holder has control in some form.

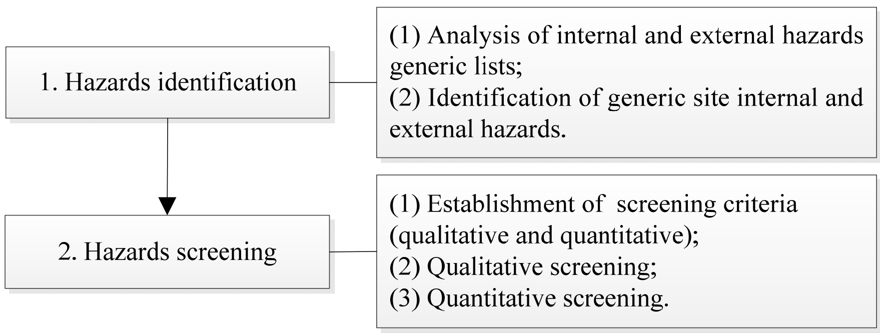
External hazards are those natural or man-made hazards to a site and facilities that originate externally to both the site and its processes, i.e. the duty-holder may have very little or no control over the IE.

Hazards can result in failure of SSCs and generate accident sequences that might lead to core damage and radioactive release. Therefore, the risk of hazards should be analysed for UK HPR1000 PSA.

14.4.2.1 Hazards Identification and Screening

Identification and screening of hazards are the first steps in the hazards PSA, and the methodology applied is adopted from Reference [16] and Reference [17].

A simplified flowchart for identification and screening of hazards is shown in F-14.4-2, which refers to Reference [16].



F-14.4-2 Simplified Flowchart for Identification and Screening of Hazards

14.4.2.1.1 Assumptions

For an Internal and External Hazards PSA, the main assumptions are listed as follows:

a) The plant design can withstand design basis loads of external hazards.

b) The impact of war, acts of sabotage or terrorism are not considered in the External Hazards PSA.

c) In addition to the above criteria, some PSA engineering experience can be used during screening. For example, where the occurrence frequency of a hazard is two orders of magnitude smaller than total CDF, or cumulative risk from screened out hazards does not exceed 1% of the total CDF.

14.4.2.1.2 Hazards Identification

According to Reference [11], the purpose of hazards identification is to obtain a complete hazards list. The steps of hazards identification used for UK HPR1000 PSA are provided as follows, Reference [16]:

a) Reference to the internationally recognised standards and references related to hazards identification and screening to develop a complete list of hazards.

b) Identification of generic site internal and external hazards in a structured framework to enable comprehensive verification.

Identification of hazards list during the GDA phase refers to international regulatory standards and references, including Reference [16], Reference [17], WENRA documents and other GDA project experience feedback. The contents of which are compared with the hazards list from the deterministic hazard analysis, Reference [23], to obtain complete lists.

To ensure the hazards list is complete, it is compared with generic site hazards information.

Internal Hazards Identification

The internal hazards list is consistent with the internal hazards list from the deterministic hazard analysis in Reference [23], which is based on Reference [16]. T-14.4-4 is the complete list of internal hazards.

T-14.4-4 Complete List of Internal Hazards

Items	Internal Hazards Description
1	Internal fire
2	Internal flooding
3	Internal explosion
4	Internal missiles
5	Dropped load

Items	Internal Hazards Description
6	Pipe whip
7	Jet impact
8	Release of fluid
9	Collapse of structures and falling objects
10	Pipe failure
11	Tanks, pumps and valve failures
12	Toxic and corrosive materials and gases
13	Water spray
14	Vehicular transport
15	Electromagnetic interference

External Hazards Identification

The external hazards list is consistent with the external hazards list from deterministic hazard analysis in Reference [23]. The external hazards list is based on References [16] , [17] and [24]. Complete list of external hazards is listed in T-14.4-5.

T-14.4-5 Complete List of External Hazards

External Hazards		
External Natural Hazards	Air based natural hazards	A01 Strong wind A02 Tornado A03 High air temperature A04 Low air temperature A05 Extreme air pressure A06 Extreme rainfall

External Hazards		
		A07 Extreme snowfall (including snowstorm) A08 Extreme hail A09 Mist A10 White Frost A11 Drought A12 Salt storm A13 Sandstorm A14 Lightning A15 Meteorite
	Ground based natural hazards	G01 Land rise G02 Soil frost G03 Animals G04 Volcanic phenomena G05 Avalanche G06 Above water landslide G07 External fire G08 Seismic hazards G09 Karsts
	Water based natural hazards	W01 Strong water current (underwater erosion) W02 Low water level W03 High water level W04 High water temperature W05 Low water temperature W06 Underwater landslide W07 Surface ice W08 Frazil ice

External Hazards		
		W09 Ice barriers W10 Organic material in water W11 Corrosion (from salt water) W12 Solid or fluid (non-gaseous) impurities from ship release W13 Chemical release to water W14 Tsunami
Man-made External Hazards		M01 Direct impact from ship collision M02 Explosion after transportation accident M03 Chemical or radiation release after transportation accident M04 Explosion outside plant M05 Explosion after pipeline accident M06 Chemical release outside site M07 Chemical release after pipeline accident M08 Missiles from military activity M09 Excavation work M10 Satellite crash M11 Aircraft crash M12 Magnetic disturbance M13 Failure of a dam upstream of the plant

Combined Hazards Identification

Potential hazards combinations that could make a significant contribution to plant risks are also considered.

Combined hazards are divided into three categories as follows:

a) Consequential hazards: This case refers to the potential for an external hazard to result in a consequential internal hazard or a consequential external hazard, such as internal flooding or external flooding following an earthquake.

b) Correlated hazards: Some external hazards which are associated with meteorological or climate conditions, intrinsically involve a combination of several phenomena. For example, more than one hazard can be derived from the same meteorological condition; a tropical cyclone may induce high wind, extreme rainfall and high waves.

c) Independent hazards combination: Independent hazards are defined as the simultaneous occurrence of two or more hazard events which have no causal relationship between them. For example there is no causal link between earthquake and temperature.

The detailed process of combined hazards identification is provided in Reference [11].

14.4.2.1.3 Hazards Screening

According to Reference [11], screening of hazards is generally established to minimise the emphasis on internal and external hazards whose significance to risk is low and to focus the analysis on hazards that are risk significant. The screening process should be applied appropriately and screening criteria should be specified to ensure that none of the significant risk contributors from any internal or external hazard relevant to the plant are not taken in to accounted

Internal Hazards Screening

The screening criteria of internal hazards refer to Reference [16] and other related references. The hazards meeting one or more of the criteria are screened out:

Criterion 1 (C1): On the basis of qualitative arguments, the hazard does not lead to an IE.

Criterion 2 (C2): The hazard is slow to develop and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate response.

Criterion 3 (C3): The hazard is included within the definition of another hazard.

Criterion 4 (C4): The hazard has a significantly lower mean frequency of occurrence than other hazards with similar uncertainties and does not result in consequences that are worse than those from other such hazards. The uncertainty in the frequency estimate for a hazard screened out in this manner is judged as not significantly influencing the total risk.

The detailed process of internal hazards screening is provided in Reference [11].

External Hazards Screening

The screening criteria of external hazards refer to Reference [17] and Reference [16]. The hazards meeting one or more of the following criteria are screened out:

Criterion 1 (C1): The hazard is of equal or less damage potential than the hazards for which the plant has been designed. This requires an evaluation of plant design bases in order to estimate the resistance of plant structures and systems to a particular hazard.

Criterion 2 (C2): The hazard has a significantly lower mean frequency of occurrence than other hazards with similar uncertainties and does not result in consequences that are worse than those from other such hazards. The uncertainty in the frequency estimate for a hazard screened out in this manner is judged as not significantly influencing the total risk.

Criterion 3 (C3): On the basis of qualitative arguments, the hazard does not lead to an IE. For external hazards, this criterion is generally applied when the hazard cannot occur close enough to the plant to affect it. Satisfaction of this criterion also depends on the magnitude of the hazard.

Criterion 4 (C4): The hazard is included within the definition of another hazard.

Criterion 5 (C5): The hazard is slow to develop and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate response.

The detailed process of external hazards screening is provided in Reference [11].

Combined Hazards Screening

The screening criteria of internal and external hazards can also be used for combined hazards.

The detailed process of screening of combined hazards is provided in Reference [11].

14.4.2.1.4 Screening Results

According to Reference [11], the screening results are divided into three categories:

a) Screened in: hazards need to be analysed during the UK HPR1000 GDA phase;

b) Unscreened: hazards need to be analysed during the UK HPR1000 nuclear site licensing phase;

c) Screened out: hazards are screened out according to screening criteria.

Screening results of hazards including internal hazards and external hazards are provided in T-14.4-6 and T-14.4-7.

T-14.4-6 Screening Results of Internal Hazards

Treatments	Internal Hazards
Screened in (in GDA phase)	Internal fire
	Internal flooding
	Dropped load
Unscreened (in nuclear site licensing phase)	Internal explosion
	Internal missiles
	High energy pipe failures
Screened out based on criteria	Release of fluid
	Collapse of structures and falling objects
	Pipe failure
	Tanks, pumps and valve failures
	Toxic and corrosive materials and gases
	Water spray
	Vehicular transport
	Electromagnetic interference

T-14.4-7 shows the screening results of external hazards, including individual external hazards and combined external hazards.

T-14.4-7 Screening Results of External Hazards

Treatments	**Hazards Group**	**Hazards Parameter**
Screened in (in GDA phase)	Air based natural hazards	A01 Strong wind A02 Tornado A07 Extreme snow (including snowstorm)
	Ground based natural hazards	G08 Seismic hazards
	Water based natural hazards	W08 Frazil ice W09 Ice barriers W10 Organic material in water
	Combined external hazards	A01 Strong wind and W10 Organic material in water A01 Strong wind and A07 Extreme snow Seismic hazards induced internal fire, internal and external or flooding External flooding
Unscreened (in nuclear site licensing phase)	Air based natural hazards	---
	Ground based natural hazards	G07 External fire
	Water based natural hazards	W03 High water level W12 Solid or fluid (non-gaseous) impurities from ship release

Treatments	Hazards Group	Hazards Parameter
	Man-made external events	M01 Direct impact from ship collision, M03 Chemical or radiation release after transportation accident M04 Explosion outside plant M06 Chemical release outside site M08 Missiles from military activity M11 Aircraft crash M12 Magnetic disturbance
Screened out based on Criteria	Air based natural hazards	A03 High air temperature A04 Low air temperature A05 Extreme air pressure A06 Extreme rain A08 Extreme hail A09 Mist A10 White frost A11 Drought A12 Saltstorm A13 Sandstorm A14 Lightning A15 Meteorite
	Ground based natural hazards	G01 Land rise G02 Soil frost G03 Animals G04 Volcanic phenomena G05 Avalanche G06 Above water landslide G09 Karsts

Treatments	Hazards Group	Hazards Parameter
	Water based natural hazards	W01 Strong water current(underwater erosion) W02 Low water level W04 High water temperature W05 Low water temperature W06 Underwater landslide W07 Surface ice W11 Corrosion (from salt water) W13 Chemical release to water W14 Tsunami
	Man-made External Events	M02 Explosion after transportation accident M05 Explosion after pipeline accident M07 Chemical release after pipeline accident M09 Excavation work off site M10 Satellite crash M13 Failure of a dam upstream of the plant

Based on the screening results of hazards, screened in hazards are analysed in UK HPR1000 GDA phase. Unscreened hazards are analysed in UK HPR1000 nuclear site licensing phase.

Internal fire, internal flooding and dropped loads are analysed during the UK HPR1000 GDA phase. Internal fire and internal flooding are addressed in Sub-chapters 14.4.2.2 and 14.4.2.3 respectively. The risk for reactor core due to a dropped load is further evaluated based on the results of the deterministic hazard analysis. The risk to the SFP posed by a dropped load is considered as part of the internal and external hazards Level 1 SFP PSA, in Sub-chapter 14.6.6.

Seismic hazard analysis is described in Sub-chapter 14.4.2.4. External flooding will be analysed and described in external flooding report. The remaining screened in external hazards (except seismic and external flooding) are described in Sub-chapter 14.4.2.5 and hazards PSA reports.

14.4.2.2 Internal Fire Level 1 PSA

14.4.2.2.1 Introduction

Internal fire occurring within nuclear power plants could cause an IE, such as a reactor trip, or affect safety functions of a system. For an internal fire Level 1 PSA, the fire risk is evaluated, and the shortfalls in fire protection are identified.

14.4.2.2.2 Scope

The scope of the UK HPR1000 internal fire Level 1 PSA is as follows:

a) Protected areas, including NI, Conventional Island (CI) and Balance of Plant (BOP).

b) Covering full power state and LPSD states.

14.4.2.2.3 Assumptions

The main assumptions of the internal fire Level 1 PSA are as follows:

a) Because cable routing information is not available during the UK HPR1000 GDA phase, cable fire ignition frequency is conservatively estimated.

b) Fire ignition source is assumed to be damaged conservatively given any fire involving itself.

c) A situation where independent fires occur in different fire compartments at the same time is not considered.

d) Passive components (e.g. tanks, pipes) are considered invulnerable to fire.

e) In fire PSA risk modelling, the assumptions are as follows:

   1) A fire will have a widespread impact within the fire compartment, and all the components of interest from the internal fire PSA in this compartment would fail. This is conservatively assumed prior to performing quantitative screening.

   2) In order to simplify the analysis and focus on the compartments that pose a significant fire risk, manual actions available to put out the fire are not considered, except for a fire in the main control room, which is conservative assumed before undertaking detailed fire modelling.

f) For the fire ignition frequency analysis, the assumptions are as follows:

   1) Fire ignition frequencies remain constant.

   2) The likelihood of fire ignition is the same across component type, regardless of size, working environment, etc.

g) In producing the fire modelling scope, the assumptions and conservatisms used are as follows:

1) Transient combustibles are not analysed, meaning they are not screened.

2) A component is considered to fail to operate normally when the environment parameter (e.g. temperature or heat flux) reaches its design threshold value, and the duration of exposure is not considered.

3) The non-suppression probability is assumed to be 1.0, which means that no suppression measure is considered.

h) In detailed fire modelling, the assumptions are as follows:

1) Fire doors remain closed during normal unit operation according to plant regulations.

2) Fire barriers can prevent fire from spreading to adjacent areas according to fire protection design requirements for single fire compartment fire scenarios.

3) If a fixed fire suppression system is available, it is assumed to be able to prevent fire growth and spread.

14.4.2.2.4 Methodology

The internal fire Level 1 PSA undertaken follows the guidance presented in Reference [25] and the requirements in Reference [17].

The methodology used for internal fire Level 1 PSA is presented in Reference [5]. The overview of the internal fire Level 1 PSA process is showed in F-14.4-3. The key elements adopted for the internal fire Level 1 PSA are as follows:

a) Plant boundary definition and partitioning;

b) Fire PSA components and cables selection;

c) Qualitative screening;

d) Fire-induced risk model;

e) Fire ignition frequencies;

f) Quantitative screening;

g) Scoping fire modelling;

h) Detailed circuit failure analysis;

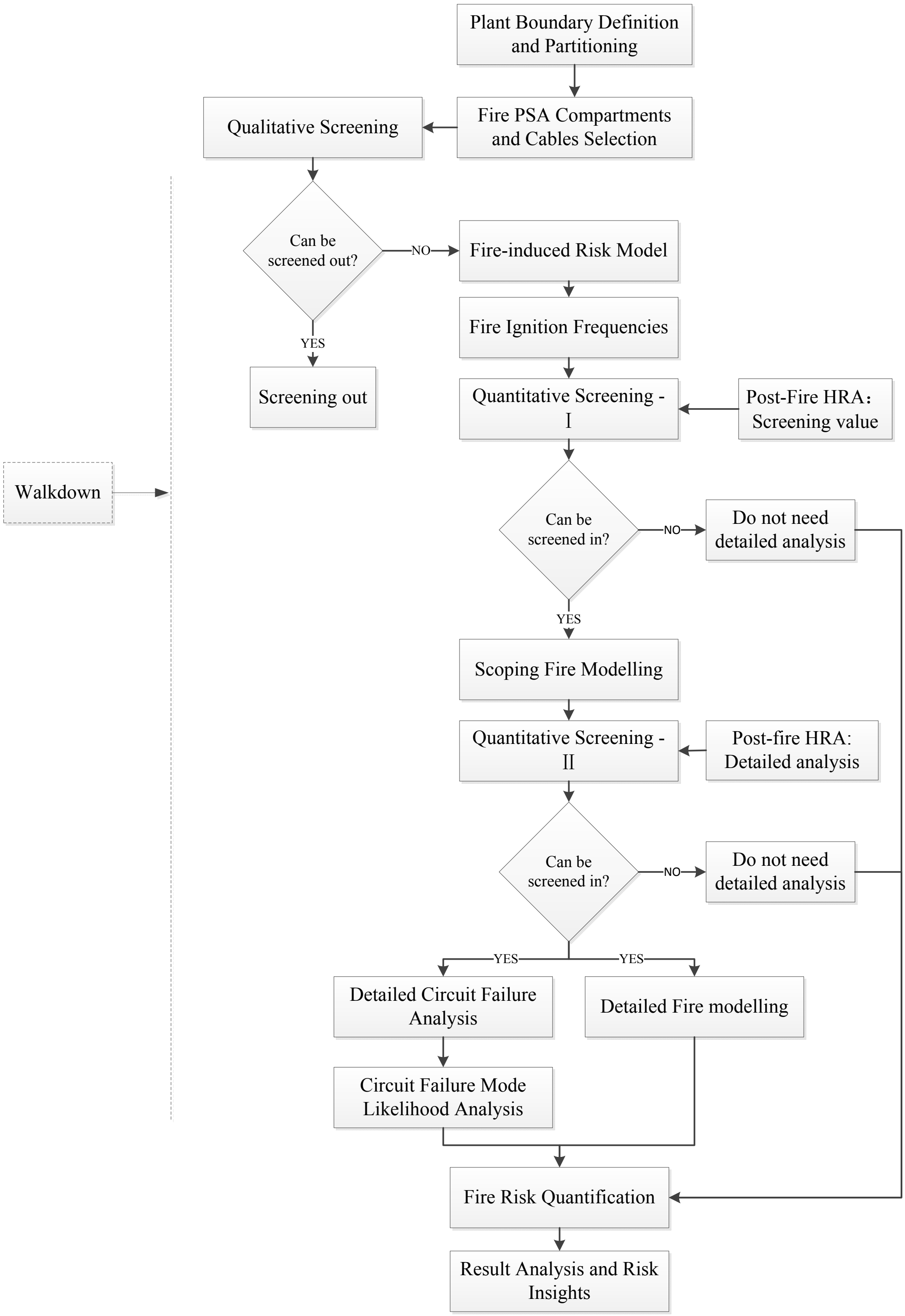
i) Circuit failure mode likelihood analysis;

j) Detailed fire modelling;

k) Fire human reliability analysis;

l) Fire risk quantification;.

m) Result analysis and risk insights.



F-14.4-3 Overview of Internal Fire Level 1 PSA Process

14.4.2.2.5 Plant Boundary Definition and Partitioning

The initial step of the internal fire Level 1 PSA is the definition of the fire compartments within the overall plant fire analysis boundary. The plant analysis boundary is defined as the areas that contain all plant contributing to normal and emergency reactor operation, associated support systems, as well as those related to power production. The plant analysis boundary is subsequently divided into a number of fire compartments with non-combustible barriers that enable these compartments to be considered independently. The partitioning principles are as follows:

a) A fire compartment is a well-defined enclosed room. Fire compartments are bounded by fire barriers where heat and products of combustion within the room are sufficiently confined.

b) If fire in one room may spread or propagate to adjacent rooms, these rooms should be grouped into one fire compartment.

c) Locations or areas free of components are neglected.

d) A location should be mapped to only one fire compartment.

e) For areas with low nuclear safety risks, such as CI and BOP, the division is made using building perimeter as the compartment boundary.

During the UK HPR1000 GDA phase, preliminary fire compartments are generally defined based on the deterministic definition of a fire area (if available). If this has not yet been defined, the whole building is considered as one fire compartment.

14.4.2.2.6 Fire PSA Components and Cables Selection

This element is used to identify the internal fire Level 1 PSA components of interest and their associated cables, and to collect necessary information relevant to other elements. The fire PSA components of interest include:

a) Components whose fire-induced failure causes an IE are modelled in the internal events Level 1 PSA.

b) Components supporting the success of mitigating safety functions are credited in the internal fire Level 1 PSA.

c) Components supporting the success of operator actions are credited in the internal fire Level 1PSA.

d) Components whose spurious actuation or other fire-induced failure modes could have an adverse effect on the success of the mitigating safety functions are modelled in the internal fire Level 1 PSA.

e) Components whose spurious operation or other fire-induced failure modes could induce inappropriate or unsafe actions by the plant operators during a fire are modelled in the internal fire Level 1 PSA.

The information includes identification of components and cables, types and locations.

Cable routing and protection features also need to be collected.

14.4.2.2.7 Qualitative Screening

The purpose of qualitative screening is to identify those fire compartments where the fire risk is expected to be relatively low or non-existent compared with others. A fire compartment could be screened out if:

a) It does not contain any fire ignition sources;

b) It does not contain safety-relevant components and associated circuits, and so, in the event of a fire, could not cause an automatic or manual trip or internal IE.

All fire compartments are evaluated one by one based on the criteria above to determine whether they can be screened out or not.

14.4.2.2.8 Fire-induced Risk Model

The fire-induced risk model is based on the internal events Level 1 PSA model, which is modified to incorporate the model changes necessary to quantify the fire risk.

A fire-induced IE is defined for each of the unscreened fire compartments identified, which is mapped to the internal IE that closely reflects the impact of the fire-induced IE in the plant. Most of these effects can be directly modelled with the existing internal events PSA accident sequence logic. Some new fire-specific sequences need to be added to the model, such as fire in main control room. The list of unscreened fire compartments following qualitative screening is reviewed to identify those components and associated failure modes and effects of concern that need to be modelled in the Internal Fire PSA.

14.4.2.2.9 Fire Ignition Frequencies

The derivation of the ignition frequencies for fire compartments considers both fixed ignition sources and transient ignition sources. The steps for calculation of ignition frequency are as follows:

a) Step 1: Ignition sources in a compartment are mapped to generic sources, and the generic frequency for each type of ignition source is taken from Reference [26].

b) Step 2: Ignition source weighting factors are calculated dividing by the number of each specific type of fixed ignition sources in a compartment by the total number of the same presented on in the plant for fixed ignition sources. For transients, three influencing factors (maintenance, occupancy and storage) are considered when calculating the weighting factor.

c) Step 3: For each type of ignition source in a compartment, an ignition frequency is determined by multiplying the generic frequency by the weighting factor, and the ignition frequency of the compartment is then the sum of frequencies of all types of ignition sources.

14.4.2.2.10 Quantitative Screening

The purpose of quantitative screening is to screen out those compartments of sufficiently low risk, and a detailed analysis is performed for remaining compartments. The screening criterion is where the sum of internal fire CDFs, for all fire compartments screened out, is less than 10% of the internal event CDF, which is taken from Reference [25].

There are two stages for quantitative screening:

a) In quantitative screening Step I, based on the fire-induced risk model and fire ignition frequencies, CDF for each fire compartment modelled is calculated. The quantitative screening criterion is then used to identify the compartments with significant risk;

b) In quantitative screening Step II, the results taken from the elements of fire modelling scoping and detailed HRA are integrated into the risk model. The quantitative screening criterion is then used to identify the compartments with significant risk.

For low risk fire compartments that are quantitatively screened out, the result is added to the total fire risk, but detailed analysis is not performed.

14.4.2.2.11 Scoping Fire Modelling

The purpose of fire modelling scoping is to screen out those fixed ignition sources that do not damage the targets of interest in a fire compartment and to assign severity factors to fixed ignition sources screened in which may reduce the compartment fire frequency.

These ignition sources are included in establishing the fire ignition frequency. Design information is required to determine related locations and other parameters (e.g., dimension, shape) of components.

14.4.2.2.12 Detailed Circuit Failure Analysis

This analysis is used to perform a deterministic failure analysis of the circuits located within unscreened fire compartments in order to identify circuits that can adversely affect the credited functionality of essential components and determine the component responses to the possible cable failure modes induced by fire damage.

Cable failure includes shorts-to-ground and hot shorts. Shorts-to-ground usually render components powered and/or controlled by this cable inoperable, and hot shorts may lead to spurious operation of components supplied. Detailed failure analysis focuses on hot shorts failure. The cables analysed mainly include power cables and control cables.

14.4.2.2.13 Circuit Failure Mode Likelihood Analysis

The purpose of this is to assign probability estimates to specific cable failure modes associated with fire-induced cable damage. According to Reference [25], there are two options for calculating circuit failure mode probabilities based on different circuit configurations:

a) Option 1: Based on failure mode probability estimate tables.

b) Option 2: Based on computational probability estimates.

14.4.2.2.14 Detailed Fire Modelling

Detailed fire modelling encompasses analysis of the physical fire behaviour (e.g. fire growth and propagation analysis), component damage, fire detection, and fire suppression. In one fire compartment, different fire scenario analyses are identified, and frequencies of occurrence are calculated using the following equation:

$$\lambda_{\mathrm{k}} = \lambda_{i,k} W_{g,k} SF_k P_{ns,k} \tag{14-1}$$

Where:

λ_{k} -- Frequency of fire scenario k (1/ (reactor year));

$\lambda_{i,k}$ -- Fire ignition frequency of the ignition source i associated with fire scenario k (1/ (reactor year));

$W_{g,k}$ -- Floor area ratio for transient fire scenario k. The floor area ratio is 1.0 for fixed ignition source fire scenarios;

SF_k -- Severity factor of fire scenario k;

$P_{ns,k}$ -- Non-suppression probability of fire scenario k;

After detailed fire modelling, the fire event trees are modified to reflect the fire scenarios.

14.4.2.2.15 Fire Human Reliability Analysis

This element is to evaluate the reliability of human actions taken in response to a fire-induced IE. The fire can increase the stress levels and workload of operators. It may also prevent operators from taking action.

The pre-fire human failure event is not included because it is not relevant once the fire has started. The human failure event that leads to fire is evaluated in the element of Fire Ignition Frequencies. The post-fire human events evaluated include existing internal event human failure events and fire-specific human failure events identified from fire-specific procedures and related training. The fire-specific human failure events mainly involve fire-related control room actions.

Manual suppression action is analysed using a suppression curve. In addition, for the element of quantitative screening, the screening value is used. For additional post-fire human events, a value of 1.0 is assigned, and for existing internal event human failure events, if the value is below 0.1, then 0.1 is conservatively chosen. Any value over 0.1 is chosen as the screening value. Human failure events which are important to risk should be analysed in detail.

The analysis focuses on the fire compartments that are screened in from quantitative screening analysis.

14.4.2.2.16 Fire Risk Quantification

This method of quantification is consistent with that introduced for the internal events Level 1 PSA to get the frequencies of accident sequences and CDF associated with fire compartments.

14.4.2.2.17 Main Results and Insights

This section will provide a summary of the internal fire Level 1 PSA results. The results and risk insights include:

a) Total internal fire CDF at full power states and LPSD states;

b) Contribution of internal fire CDF among the different fire compartments;

c) Dominant accident sequences;

d) Dominant minimal cut-sets;

e) Importance analysis results;

f) Sensitivity analysis results;

g) Uncertainty analysis results;

h) Risk insights.

14.4.2.3 Internal Flooding Level 1 PSA

14.4.2.3.1 Introduction

Internal flooding events are significant potential risks in nuclear power plants, since they represent an important class of common cause IEs. Internal flooding events are addressed in the PSA model, and treatment of these is regarded as a key element of PSA, as reflected in Reference [17].

The main purpose of the internal flooding Level 1 PSA is:

a) To assess the overall risks of internal flooding in the UK HPR1000.

b) To identify the shortfalls in internal flooding design for the UK HPR1000.

The internal flooding Level 1 PSA undertaken for the UK HPR1000 follows the guidance presented in Reference [27].

The methodology of internal flooding Level 1 PSA is presented in Reference [6].

14.4.2.3.2 Scope

The UK HPR1000 internal flooding Level 1 PSA scope is as follows:

a) The nuclear power plant production area is the main area considered in the internal flooding PSA, which includes the NI, CI and BOP.

b) It is limited to flooding within the building.

c) It covers full power state and LPSD states.

14.4.2.3.3 Assumptions

The main internal flooding Level 1 PSA assumptions include:

a) A building or room which is physically isolated can be considered as a separate flooding area. If there is no physical isolation between adjacent rooms, they can be merged into one flooding area.

b) Corridors or opening areas outside the building are not considered as a flooding area.

c) For areas with low risk, such as the CI and BOP, the analysis is performed at a building level.

d) It is conservatively assumed that the failure of an SSC is caused by a flooding event or major flooding event without considering the flooding water height.

e) The occurrence of flooding events can cause the failure of electrical equipment in the flooding areas.

f) For passive components (e.g., heat exchangers, check valves, manual valves) or other components that do not need to change position or operate using external power, it is considered that a flooding event does not affect their availability.

g) It is assumed that electrical motor valves fail during a flooding event and thus remain in their original position.

h) If flooding causes the failure of pneumatic valves, the valves are in the fail-to-safe position following gas loss and cannot be adjusted; this is also true for pneumatic regulating valves.

i) The expected consequence of flooding and major flooding of electrical equipment (e.g., control cabinets, electrical cabinets and terminal boxes) is a ground short circuit, which causes the load supplied by the equipment to lose power.

j) It is conservatively assumed that devices fail due to spray should the degree of protection provided by enclosure of the device not be adequate;

k) It is supposed that water-spray causes electrical equipment (e.g., switches) to fail unless the equipment is protected by an appropriate shield or enclosure.

l) If oil is sprayed into pumps or valve motors, according to the characteristics of the oil, it does not cause damage as long as the oil has been purified. Even if the oil is sprayed into the motor winding, it only affects the insulation of the winding without causing a short circuit between phases. Oil sprayed into the motors does not affect the availability of the motors.

m) It is considered that spray has no effect on the availability of the electric valves, because electrical motor valves will have an appropriately-sealed waterproof shell, and the interface between the cable and electric head will feature plastic sealing.

n) If there is the requirement for unit shutdown within 24 hours as a result of SSC failure caused by a flooding event, it is conservatively assumed that the unit should be shut down manually; therefore, a transient condition is caused by the SSC failure resulting from flooding events.

o) Multiple independent internal flooding events caused by different flooding sources in the same time are not considered in the internal flooding Level 1 PSA.

p) Other IEs such as LOOP coincident with flooding are not taken into account.

14.4.2.3.4 Methodology

The internal flooding Level 1 PSA follows the guidance presented in References [27] and [17]. The key steps adopted are as follows:

a) Flooding information identification;

b) Qualitative screening;

c) Flooding scenarios analysis;

d) Flooding consequence analysis;

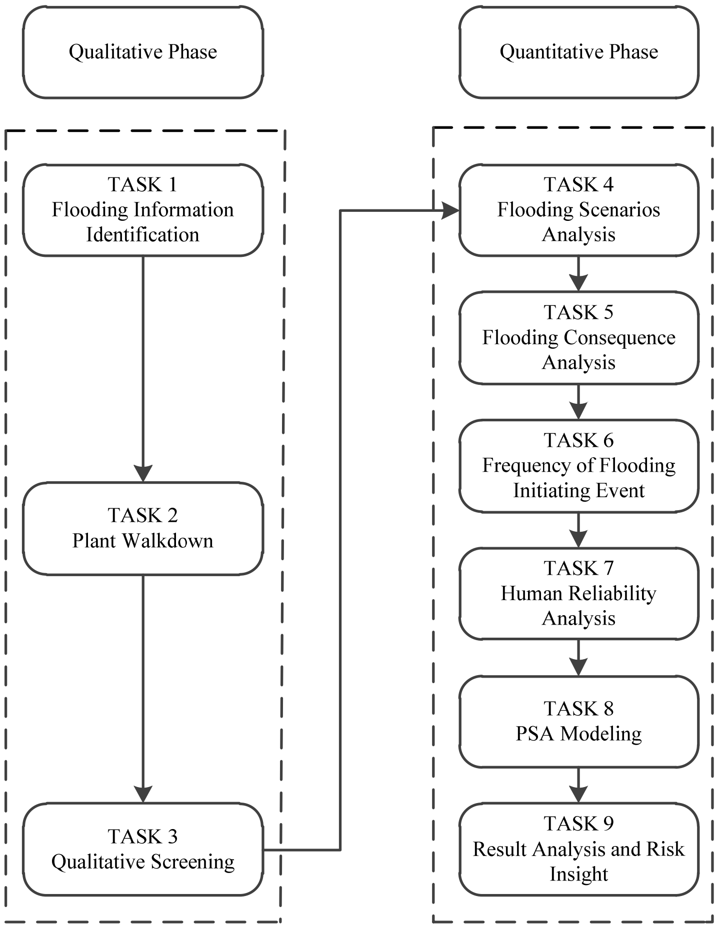
e) Frequency of calculation flooding IE;

f) Human reliability analysis;

g) PSA modelling;

h) Result analysis and risk insights.

The methodology used for internal flooding Level 1 PSA can be divided into two phases (shown in the F-14.4-4): qualitative phase and quantitative phase. Tasks 1 to 3 belong to the qualitative phase, and the others belong to the quantitative phase.



F-14.4-4 Major Tasks in the Methodology of Internal Flooding Level 1 PSA

14.4.2.3.5 Flooding Information Identification

The purpose of this task is to identify the flooding information, and the information includes flooding areas, flooding sources and SSCs affected by flooding.

a) Flooding Areas Identification

The process of flooding area identification is as follows:

1) Obtain a list of all NI, CI and BOP buildings and rooms and use it as a preliminary list of flooding areas.

2) Revise the preliminary list of flooding areas according to design information, and then obtain a final list of flooding areas.

b) Flooding Sources Identification

Plant systems that convey fluid through any area are considered as potential flooding sources. For each selected flooding area, the following flooding sources, as listed in Reference [27], should be included in the analysis.

1) Equipment (e.g., piping, valves and pumps) from a fluid system, either operational or on standby, located in the area.

2) Ingress from other flooded areas (e.g., back flow through drains or doorways).

c) SSCs affected by Flooding Identification

The SSCs located in each of the flooding areas and along the propagation paths need to be identified to from an SSC list. According to Reference [27], the principles of identifying the SSCs located within these areas are as follows:

1) SSCs are required to respond to an IE, or failure of an SSC challenges normal plant operation.

2) SSCs whose failure potentially causes IEs.

For each identified SSC, it is necessary to identify its spatial location in the flooding area for the purposes of qualitative screening.

14.4.2.3.6 Plant Walkdown

Plant walkdown are required to verify the accuracy of the information identified in task 1; this task is not applicable at this stage of the GDA.

14.4.2.3.7 Qualitative Screening

The purpose of this task is to identify all credible, safety-significant flooding scenarios. Each flooding area must be reviewed to determine whether it can be screened out from further evaluation by various screening criteria.

The qualitative screening criteria are as follows:

a) Screen out the areas free from flooding sources and propagation potential;

b) Screen out the potential flood areas which cannot result in an IE or need for immediate plant shutdown if flooded.

c) Screen out the potential flooding areas which cannot potentially impact safety critical SSCs if flooded.

Flooding areas not screened out are analysed in detail during the quantitative phases.

14.4.2.3.8 Flooding Scenarios Analysis

After qualitative screening, the remaining flooding areas need to undergo detailed analysis including identification of the flooding types and analysis of the results of potential SSC failure.

In the internal flooding Level 1 PSA, three types of flooding are considered: spray, flooding and major flooding. According to Reference [27], there are three identification criteria:

a) Spray leak or flow rate is in excess of $0.2271 m^3/h$ but typically less than $22.71 m^3/h$.

b) The flow rate of flooding event is in excess of $22.71 m^3/h$ but no larger than $454.2 m^3/h$.

c) The flow rate of major flooding event is excess of $454.2 m^3/h$.

14.4.2.3.9 Flooding Consequence Analysis

Flooding consequence analysis based on the flooding scenario analysis is used to evaluate the impact of flooding height on the availability of important SSCs. Furthermore, internal IEs caused by each flooding event are obtained using the internal events Level 1 PSA.

14.4.2.3.10 Flooding Initiating Event Frequency

The purpose of this task is to identify the flood- induced IEs in the remaining flooding areas which need quantification analysis and estimate their frequencies. The majority of flood-induced initiating events involve pipe failure, but maintenance-induced and other human error events are also considered.

14.4.2.3.11 Human Reliability Analysis

a) Type A Human Failure Events

The analysis methodology for type A human failure events provided in Reference [4] is appropriate for significant systems related to the internal flooding PSA. However, the step for "Systems Identification" as part of the analysis method should first be used to identify the systems of significance.

b) Type B Human Failure Events

Analysis of type B human failure events for the internal flooding PSA used statistical data drawn from relevant operating experience and the random nature of flooding when associated with human error.

c) Type C Human Failure Events

The analysis of type C human failure events focusses on the assessment of reliability for human activities taken in response to a flood-induced IE. The flooding event can increase the stress levels and workload of operators, and it may also prevent operators from taking appropriate action.

The type C human failure events in the internal flooding Level 1 PSA include type C human failure events from the internal event Level 1 PSA, and type C human failure events identified from flood-specific procedures and training.

14.4.2.3.12 PSA Modelling

The process of developing the internal flooding Level 1 PSA model includes three steps:

a) Develop the internal flooding Level 1 PSA pre-event trees

Internal flooding Level 1 PSA pre-event trees are developed using the corresponding flooding areas screened in.

b) Link the internal flooding Level 1 PSA pre-event trees to the internal events Level 1 PSA model

According to flooding consequence analysis, the IEs resulting from flooding events can be identified, and these IEs can be used to link the internal flooding PSA pre-event trees to the internal events Level 1 PSA model.

c) Develop boundary condition

SSC failure is assumed in the flooding areas screened in; therefore, the relevant basic events are set to “TRUE” when defining the boundary conditions.

14.4.2.3.13 Main Results and Risk Insights

The purpose of this task is to perform quantification of flood-induced accident sequences. After all of the technical elements will be modelled in the internal flooding Level 1 PSA, the quantification process can be performed.

The main results and risk insights for the internal flooding Level 1 PSA will include:

a) Total internal flooding CDF at full power state and LPSD states;

b) Contribution of CDF by different flooding areas;

c) Dominant core damage sequences;

d) Dominant minimal cut-sets;

e) Importance analysis results;

f) Sensitivity analysis results;

g) Uncertainty analysis results;

h) Risk insights.

14.4.2.4 Seismic Level 1 PSA

14.4.2.4.1 Introduction

The objective of the seismic PSA is to evaluate the seismic risk of the plants, assess the plant response to earthquake, evaluate balance of seismic design, and identify seismic design weaknesses which may be improved.

The seismic PSA methodology for UK HPR1000 is done according to Reference [28] and employs relevant experience provided in Reference [17].

14.4.2.4.2 Methodology

The overview of the seismic PSA process is showed in F-14.4-5.The following tasks are determined based on the key elements:

a) Seismic hazard analysis.

b) Seismic Equipment List (SEL) Development.

c) Floor spectra and structural response development.

d) Seismic capacity screening.

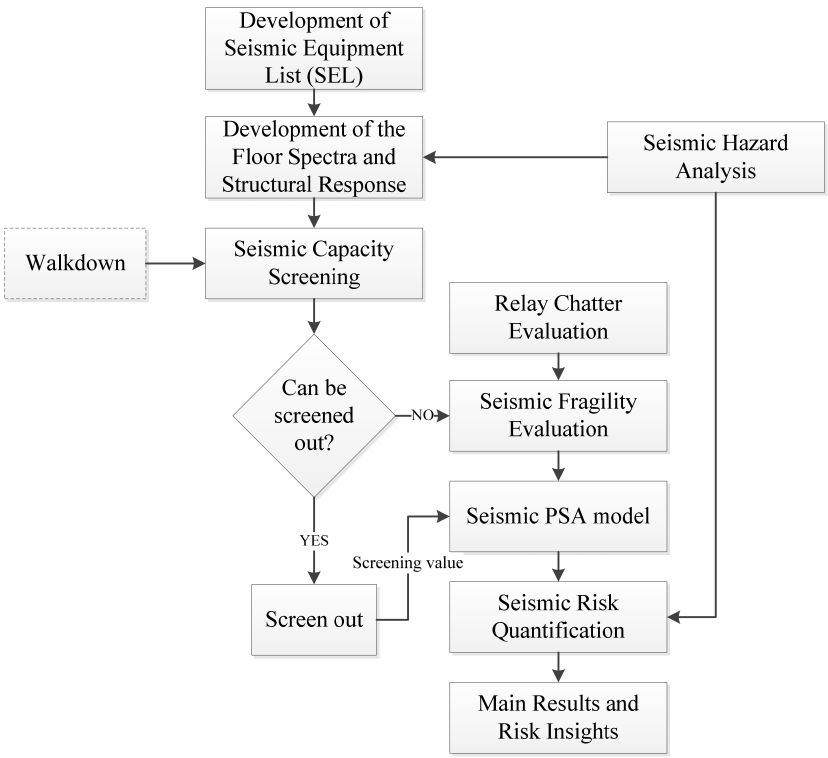
e) Relay chatters evaluation.

f) Seismic fragility evaluation.

g) Seismic PSA model.

h) Seismic risk quantification.

i) Result analysis and risk insights.



F-14.4-5 Overview of Seismic Level 1 PSA Process

Seismic Hazard Analysis

Seismic hazard analysis can determine an appropriate hazard curve that provides information regarding the annual frequency for different levels of Peak Ground Acceleration (PGA).

It is noted that the curves are involved to continuous range of PGA. The hazard curves should be divided into several sub-intervals which indicate as different seismic initiators to develop seismic PSA model and quantify the seismic risk.

Seismic Equipment List Development

SEL is vital for demonstrating completeness of the seismically-initiated sequences considered in the seismic PSA. The initial SEL comes from the following:

a) Equipment modelled in the internal events Level 1 PSA model;

b) Both active (pumps, valves, etc.) and passive (water tank, pipe, cabinets, etc.) equipment. The passive equipment is perhaps screened out from the internal events Level 1 PSA model but its seismically induced failure could affect safety functions;

c) Equipment where seismic failure may affect post-initiator operator action pathways or normal operation of other safety equipment;

d) Equipment where seismic failures may affect other structures/equipment on the SEL;

e) Sources of fire and flooding, and the equipment which needs to mitigate seismic-induced fire and flooding;

f) Equipment in non-safety systems credited for safe shutdown;

g) Structures (e.g. the reactor building) containing the above equipment.

As the seismic PSA is developed, additional equipment may need to be added to the SEL to ensure there are no omissions. Equipment information includes, but is not limited to, coding, description, function, location and seismic level.

Floor Spectra and Structural Response Development

This task aims to develop realistic floor spectra and structural response based on seismic hazard analysis. It is a necessary input for the fragility evaluation.

Usually, the ground response spectrum used as an input for this task is the median spectral shape for a 10,000-year return period.

Seismic Capacity Screening

In order to reduce the workload for calculating the fragilities of SSCs and focus on analysis for low seismic capacity equipment, certain high seismic capacity equipment is screened out from the SEL.

The screening guidance is based on table 2-3 and table 2-4 from Reference [29] in terms of five percent damped peak spectral ground acceleration.

The screening is based on the seismic hazard curves and the associated conditional probability of failure of SSCs with fragility corresponding to the screening level. The High Confidence of Low Probability of Failure (HCLPF) of SSCs is used to support screening. The HCLPF level of screening is chosen so that the screened out equipment is not significant to the seismic CDF.

Relay Chatter Evaluation

Relay chatter during an earthquake which is considered a unique failure mode could result in adverse effects on plant safety. The relays evaluated are related to equipment in the SEL. Relay chatter can cause the unavailability of equipment, operator confusion, and containment bypass events.

A screening process is performed to evaluate relay chatter. The relays whose failure cannot affect the operation of associated systems, or those with very high seismic resistance are screened out.

Seismic Fragility Evaluation

Structure or equipment may be associated with multiple failure modes, and the main failure mode is evaluated. The evaluation undertaken follows the guidance presented in Reference [30].

This evaluation is used to estimate the conditional probability of failure of a structure or equipment for a given value of seismic ground motion. The results are shown as the family of seismic fragility curves, which is expressed by the median acceleration seismic capacity (A_m), logarithmic standard deviations reflecting randomness in seismic capacity (β_R), and uncertainty in the median seismic capacity (β_U).

The fragility can be represented by the following equation from Reference [30] and Reference [28]:

$$f' = \Phi\left(\frac{\ln\left(\frac{a}{A_m}\right) + \beta_U \Phi^{-1}(Q)}{\beta_R}\right) \tag{14-2}$$

Where:

Q--P [f< $f'|a$], that is, the subjective probability (confidence) that the conditional probability of failure, f, is less than $f'$for a PGA a.

a -- Given value of seismic ground motion (e.g., PGA).

Φ -- Standard Gaussian cumulative distribution.

Φ^{-1}-- Inverse of the standard Gaussian cumulative distribution.

Seismic PSA Model

The seismic PSA model is completed based on the internal events Level 1 PSA model, by modifying event trees and fault trees to reflect seismic effects.

Seismic Induced Initiating Events Analysis

Earthquakes disturb the normal operation of the nuclear power plant. This analysis uses a seismic-induced IE tree to disposition the more pervasive effects of a seismic event that can directly lead to core damage or to an IE modelled in internal events Level 1 PSA model.

Seismic Induced Accident Sequences Analysis

The seismically-induced accident sequences are developed for each IE tree end state. The analysis uses event trees that are similar in content and structure to event trees developed for the internal events Level 1 PSA model.

Seismic Fault Trees Analysis

The seismic fault tree is based on the internal events Level 1 PSA system fault trees. The seismic fault tree includes random failure events and seismic failure events. Some SSCs (e.g., structures, passive equipment and tanks) and failure modes are added to the seismic fault tree.

Human Reliability Analysis

This analysis focuses on the post-initiator operator actions, and the pre-initiator operator actions are not affected by an earthquake. It is noted that seismic events can influence the success of operator actions to a great extent compared to normal situations.

HEP is considered with alongside specific factors to identify the influence of seismic events on operator actions, such as:

a) Time after the seismic event;

b) Location of the operator action;

c) Earthquake severity.

Seismic Dependency Analysis

Seismic events affect the total plant, and can easily cause redundant SSC failure. Therefore, dependency between SSC failures is considered.

Seismic Risk Quantification

Seismic risk quantification is derived from the combination of the seismic PSA model, SSC fragilities and seismic hazard curves. Both seismic hazard curves and SSC fragility curves are composed of different confidence curves. The Monte Carlo Simulation method is used to quantify the uncertainty.

14.4.2.4.3 Seismic Risk Insights

The risk insights of seismic will be described in Risk Insights of Seismic PSA for UK HPR1000 Report.

14.4.2.5 External Hazards Level 1 PSA

14.4.2.5.1 Introduction

Screened-in external hazards (excluding seismic) which impact SSCs and potentially degrade one or more plant safety function and, at the same time, challenge plant safety systems that act to keep the plant in a safe state or bring it to a safe state are analysed in the scope of the external hazards Level 1 PSA.

Based on the results of screening, the analysis of external hazards includes bounding analysis and detailed analysis.

The objectives of the external hazards analysis are to quantify the risk of external hazards that could lead to core damage and to provide additional measures to reduce risk.

The external hazards Level 1 PSA follow the guidance presented in Reference [16] and Reference [17].

14.4.2.5.2 Scope

The analysis focuses on the external hazards Level 1 PSA that focusses on reactor core damage. The scope of the UK HPR1000 external hazards Level 1 PSA includes full power and LPSD states.

14.4.2.5.3 Assumptions

The main assumptions are as follows:

a) Because plant response procedures for external hazards are not available during the GDA phase, plant response procedures for external hazards are drawn from engineering experience feedback.

b) During hazard analysis, if generic hazards data, Reference [24], are not available, conservative data is assumed.

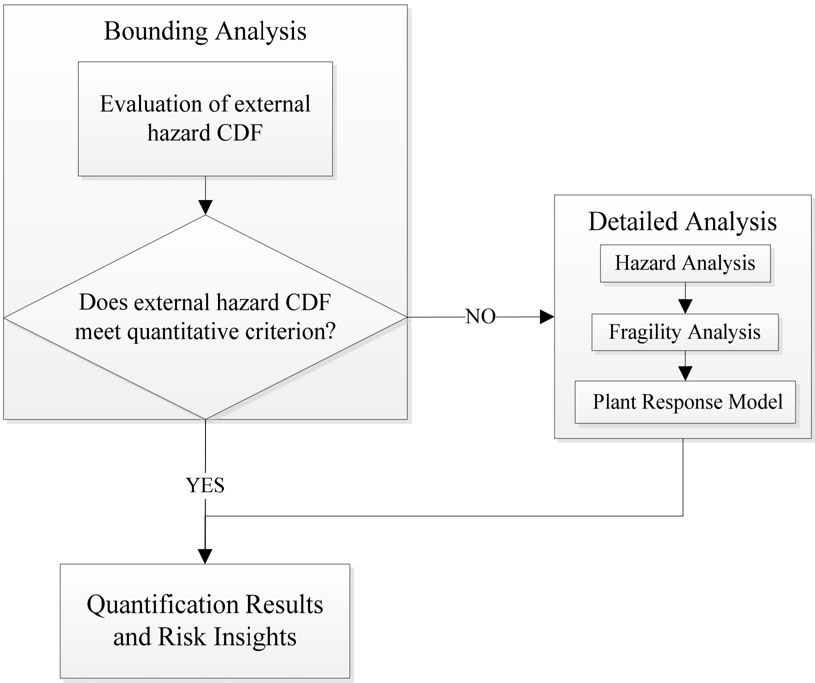
c) For the fragility analysis, if suitable methodology, generic site information or equipment specific information are not available, equipment fragility values are estimated using conservative assumptions and expert judgement.

14.4.2.5.4 Methodology

The risk of external hazards can be evaluated using a bounding or detailed analysis to characterise the hazards and to reflect the potential threat from these in the PSA models for significant hazards.

The analysis procedure for the external hazards Level 1 PSA is shown as below in F-14.4-6.

Detailed methodology of the external hazards PSA is provided in Reference [7].



F-14.4-6 Analysis Procedure for External Hazards Level 1 PSA

14.4.2.5.5 Bounding Analysis

Bounding analysis is a conservative quantification method, which is performed with the aim of reducing the list of external hazards subject to detailed analysis.

In the bounding analysis, all potential impacts of each screened-in external hazard are considered.

In the bounding analysis, the external hazard CDF is the product of external hazard initiating frequency and simplified Conditional Core Damage Probability (CCDP). The general formula for calculating the bounding analysis results from an external hazard is:

$$f_{\text{External hazard CDF}} = f_{\text{Hazard in Plant Area}} \times CCDP \qquad (14\text{-}3)$$

Where:

$f_{\text{External hazard CDF}}$ --The CDF contribution from the external hazard.

$f_{\text{Hazard in Plant Area}}$ --The occurrence frequency of the external hazard.

CCDP: CCDP for an external hazard, which is estimated based on either the CCDP of internal IEs for the internal events Level 1 PSA, or conservative assumptions.

According to Reference [16], the quantitative criteria for the bounding analysis depends on the overall objective of the internal events Level 1 PSA and correlates with the CDF from internal events, and the internal and external hazards Level 1 PSA.

Based on Reference [16] and engineering experience, quantitative criteria for the bounding analysis is that the external hazard CDF is less than 1E-08/ reactor year, which is two orders of magnitude lower than the overall objective in the internal events Level 1 PSA.

If, following bounding analysis, the external hazards CDF meets the quantitative criteria, the external hazards CDF is retained in the final results of the external hazards PSA. If the CDF of external hazards does not meet the quantitative criteria, a detailed analysis will instead be carried out.

14.4.2.5.6 Detailed Analysis

Detailed analysis is performed for screened in external hazards, where the CDF, following bounding analysis, does not meet quantitative criteria.

As stated in Reference [17], detailed analysis includes hazard analysis, fragility analysis and plant response modelling.

Hazard Analysis

The objective of hazard analysis is to estimate the occurrence frequency of external hazards as a function of external hazard intensity.

In the UK HPR1000 PSA, hazard analysis is based on the probabilistic evaluation reflecting generic hazards data in Reference [24]. If generic hazards data are not available, conservative data are assumed for analysis and a sensitivity analysis is performed.

Fragility Analysis

The objective of the fragility analysis is to identify SSCs that are susceptible to the effects of external hazards and to determine conditional failure probabilities as a function of external hazard intensity.

The fragility analysis of SSCs is based on generic site and SSC specific information.

Plant Response Model

The analysis steps for the plant response model are as follows:

a) Initiating events analysis

The major impacts of external hazards, that could directly lead to core damage or that challenge normal operation and which requires successful mitigation using safety or non-safety systems to prevent core damage, are assessed using hazard initiating event trees.

b) Accident sequence analysis

Accident sequence analysis is assessed by modifying appropriate event trees from the internal events Level 1 PSA model to reflect specific impacts of external hazards.

c) System analysis

Fault trees from the internal events Level 1 PSA, which are used in mitigation of external hazards, are modified to reflect the specific impacts of external hazards (e.g. by adding component failure modes caused by external hazards).

d) Human reliability analysis

External hazards can increase the likelihood of human errors, when compared to internal events.

Human failure events that lead to external hazards are considered under the occurrence frequency of external hazards.

Post-hazard human failure events are considered in the external hazards Level 1 PSA, which is to evaluate the reliability of human actions during the mitigation of external hazards.

e) Quantification

Detailed analysis quantification appropriately integrates the hazard analysis, SSC fragilities analysis and external hazards PSA model.

14.4.2.5.7 Main Results and Risk Insights

The PSA quantification results include the most significant contributors to CDF, such as the CDF for each external hazard, dominant accident sequences and dominant minimal cut-sets. Uncertainty analysis results, importance analysis results, and sensitivity analysis results are also provided as a supplement for the comprehensive understanding of the plant risks.

External hazards Level 1 PSA results will include:

a) Total CDF from external hazards;

b) Contribution of CDF resulting from different kinds of external hazards;

c) Contribution of CDF at full power state, LPSD states;

d) Lists of dominant accident sequences and dominant minimal cut-sets;

e) Importance analysis results;

f) Sensitivity analysis results;

g) Uncertainty analysis results;

h) Risk insights.

14.5 Level 2 PSA

14.5.1 Introduction

The Level 2 PSA is developed to assess the response of systems and components fulfilling containment and other functions to potential loads and to assess the characteristics of a radiological release during a severe accident. Frequency, composition, magnitude, and timing of fission product releases, etc., are calculated in the Level 2 PSA. The results gained are important when assessing against radiation protection targets 5 and 6 and are used as inputs to the Level 3 PSA.

14.5.2 Scope

The scope of the UK HPR1000 Level 2 PSA for reactor core includes:

a) All POSs identified for the Level 1 PSA for reactor core, including:

    1) Full power state.

    2) LPSD states.

b) All IEs analysed in the Level 1 PSA for reactor core:

    1) Internal events.

    2) Internal hazards.

    3) External hazards.

Level 2 PSA for the SFP is provided in Sub-chapter 14.6.7.

14.5.3 Assumptions

The main assumptions for the Level 2 PSA are as follows:

a) The availability and reliability of equipment claimed for severe accident mitigation are assumed to be unaffected under severe accident conditions in accordance with their qualification and based on international good practice.

b) In Level 2 PSA mission times of 24 hours are sufficient for the implementation of the majority of required mitigation functions, with the exception of long-term mitigation. Mission times of less than 24 hours are only used for components dedicated to maintaining the power supply (e.g., batteries dedicated to severe accident conditions). A sensitivity analysis for components with mission times of more than 24 hours is carried out to evaluate the effect on the risk.

14.5.4 Methodology

The Level 2 PSA for the UK HPR1000 follows the guidance presented in Reference [31] and Reference [32].The key steps adopted are as follows:

a) Level 1/Level 2 PSA interface analysis.

b) Severe accident progress and containment response analysis:

1) Severe accident progress analysis.

2) Containment structure performance analysis.

3) Severe accident phenomena probability analysis.

c) Containment Event Tree (CET) construction and quantification.

d) Other supporting elements analysis:

1) System analysis.

2) Human reliability analysis.

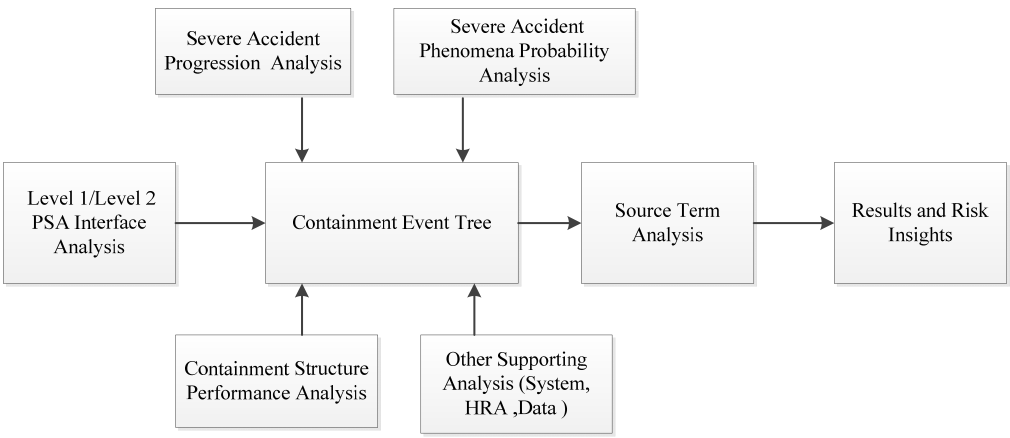
3) Data analysis.

e) Source terms analysis.

f) Quantification analysis and risk Insights.

The detailed analysis methodology for Level 2 PSA technical elements is in Reference [8].

The main technical elements and their relationships within the Level 2 PSA are shown in F-14.5-1.



F-14.5-1 Main Technical Elements of Level 2 PSA

14.5.5 Level 1/Level 2 PSA Interface Analysis

The primary objective of the Level 1/Level 2 PSA interface analysis is to provide an effective transfer of information between the Level 1 PSA CDF evaluations and the core melt progression analysis that is conducted as part of the Level 2 analysis.

The quantification of the Level 2 PSA is undertaken using the Risk Spectrum professional software (version 1.2.1) allowing for clear and transparent demonstration of the link between the Level 1 core damage sequences and their further analysis in the Level 2 PSA.

A set of Plant Damage State (PDS) is defined to enable the core damage events identified in the Level 1 PSA report to be grouped in a way that facilitates the accurate treatment of severe accident phenomena in the Level 2 PSA. These PDSs are defined according to plant characteristics that define the status of the plant at the time of core damage. A PDS therefore represents a group of sequences that are considered likely to have similar accident progressions.

The definition of PDS applied to the UK HPR1000 Level 2 PSA is based on the attributes presented in Reference [31]. However, characteristics related to systems are put in the CETs function events, such as the state of Steam Generator (SG), Containment systems, RIS, Containment Heat Removal System (EHR [CHRS]).

The following PDS characteristics have been determined in the UK HPR1000 Level 2 PSA, shown in T-14.5-1. The proposed PDSs are presented in T-14.5-2.

T-14.5-1 Characteristics and Attributes of PDS

Characteristics	Attributes
Types of IEs	Bypass (Interfacing systems Loss of Coolant Accident (ISLOCA)/ SGTR))
	LOCA (large break, intermediate break and small break)
	Transients (representing IEs with intact primary loop and secondary loop)
Pressure of primary loop	High pressure
	Low pressure
Integrity of secondary loop	Integrated
	Break

Characteristics	Attributes
State of alternating current (AC) power supply	Normal
	Can be restored
	Cannot be restored

T-14.5-2 Proposed UK HPR1000 Level 2 PSA Plant Damage States

PDS	Description
POS A	
LL	Large break / intermediate break LOCA core damage sequences
SL	Small break LOCA core damage sequences with primary loop at high pressure
IS	ISLOCA core damage sequence
TR	Transients core damage sequences with primary loop at high pressure
VS	Main steam/feed water pipe break core damage sequences with primary loop at high pressure
SLD	Small break LOCA core damage sequences with primary loop at low pressure
SG	SGTR core damage sequences isolated successfully with primary loop at high pressure
SS	SGTR non-isolated core damage sequences
VR	RPV large break core damage sequences
AT	Anticipated Transient Without Scram (ATWS) core damage sequences with primary loop at high pressure
TP	Station black out core damage sequences with primary loop at high pressure
LPSD states (POS B/ POS C/ POS D/ POS G)	
LL_S	Large/ intermediate break LOCA core damage sequences in LPSD
SL_S	Small break LOCA core damage sequences with primary loop at high pressure in LPSD states
IS_S	ISLOCA core damage sequence in LPSD states

PDS	Description
TR_S	Transients core damage sequences with primary loop at high pressure in LPSD states
VS_S	Main steam/feed water pipe break core damage sequences with primary loop at high pressure in LPSD states
SLD_S	Small break LOCA core damage sequences with primary loop at low pressure in LPSD states
SG_S	SGTR isolated successfully core damage sequences with primary loop at high pressure in LPSD states
SS_S	SGTR non- isolated core damage sequences in LPSD states
TP_S	Station black out core damage sequences with primary loop at high pressure in LPSD states

14.5.6 Severe Accident Progression Analysis

The severe accident progression analysis is used to evaluate the progression of events and provide information on severe accident behaviour and containment response.

Calculations are performed for the PDSs that are significant contributors to CDF. PDSs that may have a small occurrence frequency but have the potential to result in large and/or early releases of radioactive material to environment are also included. Such PDSs typically involve either direct containment bypass or early failure of the primary and/or secondary containments.

14.5.7 Severe Accident Phenomenon Analysis

The severe accident phenomena considered in the Level 2 PSA are as follows:

a) Induced reactor coolant pressure boundary break;

b) In-Vessel Retention (IVR);

c) Primary water injection (core re-flooding);

d) Hydrogen combustion and explosion;

e) Fuel-coolant interaction (steam explosion);

f) Molten Core-Concrete Interaction (MCCI);

g) Containment overpressure;

h) Phenomena at the time of RPV failure (overpressure of the reactor pit, RPV rocketing, Direct Containment Heating (DCH)).

Probabilities of the phenomena above are calculated using the risk-orientated accident analysis methodology combined with either the sampling method or engineering judgment based on the design of the UK HPR1000. Methods chosen are used in conjunction with either the interpretation of the deterministic severe accident or the reference data from the research of the similar NPPs.

14.5.8 Containment Structural Performance Analysis

The objective of containment structural performance analysis is to develop a fragility curve for containment. The analysis steps are listed as below:

a) Use the finite element analysis software to establish an overall model of the containment. The model includes the containment design features such as equipment and personnel hatches, pre-stressed components and the steel liner. Considering the nonlinear characteristics of materials, appropriate units are used to simulate the materials and structural elements such as concrete, steel liner, reinforcement and pre-stressed components, etc.

b) Adopt the Latin Hypercube Simulation procedure to generate certain sets of random parameters to be used as the input into the analytical models of the containment.

c) Input the parameters from the previous step into the analytical model to analyse the containment at different internal pressures. The ultimate containment capacity for each sample is determined and then statistical analysis is performed to obtain its distribution function.

d) Form the initial probabilistic fragility curve according to the results of the previous step.

e) Calculate the ultimate capacity considering temperature load.

f) Revise the probabilistic fragility curve according to the calculation results based on temperature load.

14.5.9 Containment Event Tree

The core damage sequences to be evaluated are identified by PDS grouping, and plant response to various accident sequences obtained by analysis of accident progress. PDSs are used as the input for establishing logic models for accident development. This model is presented in the form of an event tree and often called a CET.

The construction and quantification of CETs in the Level 2 PSA is similar to the methods used for Level 1 PSA ETs creation, and the following 2 points should be noted:

a) Consideration of chronological order. The event tree is typically established in chronological order, as with the Level 1 PSA. Level 2 PSA event trees generally include three stages:

   1) T1: the stage before RPV failure.

2) T2: the time of RPV failure.

3) T3: a significant length of time after RPV failure.

The time between core melt to RPV failure ranges from approximately 2h~3h up to 10h~20h. Accident progress and phenomena before and after RPV failure vary significantly. The challenges posed to maintaining containment after RPV failure are usually considered to be medium-term to long-term effects.

b) Since there are possibly some function events with higher failure probabilities than others within the Level 2 PSA, logic and simple quantitative analysis of the success state are used.

During the development of the of CET, in order to facilitate model quantification and avoid extensive repetition, boundary conditions and house events are used to distinguish time windows and success criteria for different PDS groups. For most of the PDS groups, severe accident progression and mitigation are similar except for PDS groups considered under different primary loop pressures. Therefore, high pressure CETs and low pressure CETs are constructed and combined with boundary conditions and house events. Some significant PDS groups, such as PDS with containment bypass and RPV rupture, are treated with a single CET. So the PDSs are linked to five different CETs, including:

1) High pressure CET.

2) Low pressure CET.

3) SGTR CET.

4) ISLOCA CET.

5) RPV failure CET.

Severe accident mitigation functions and operator actions included in the CETs are listed as follows:

a) Containment isolation

Containment isolation is carried out automatically or manually to ensure that the fission products do not leak out through containment penetration if valves on the penetration pipe are closed.

b) Primary loop depressurisation

Primary system depressurisation is achieved using Severe Accident Dedicated Valves (SADVs) which effectively prevent a high-pressure core melt accident by opening within the required time during a severe accident, lowering the primary pressure to below 2.0 MPa abs.

This function event is specific to the high pressure CET.

c) Reactor cavity water injection

Reactor cavity water injection is carried out using the EHR [CHRS] via both passive and active injection into the reactor cavity for in-vessel corium retention.

d) Reactor core re-flooding

The water is injected into the reactor core using the RIS [SIS] for reactor core re-flooding.

e) Containment heat removal

Residual containment heat is removed using the EHR [CHRS] and Extra Cooling System (ECS [ECS]).

f) Passive hydrogen recombiner

Passive autocatalytic recombiners are effective when the hydrogen concentration reaches 2% (by volume). In addition, five hydrogen sensors are located in the appropriate locations within the containment to indicate the hydrogen risk posed in conjunction with the pressure measured. The failure probability of the passive hydrogen recombiners is considered to be very low.

14.5.10 Other Supporting Analysis

Other supporting analysis refers to the technical elements included in Level 1 PSA which are not special to Level 2 PSA, such as system analysis and HRA. HRA of Level 2 PSA is carried out according to the severe accident management strategy. The dealing manner is given in Reference [8].

14.5.11 Radiological Source Term Analysis

The source terms associated with the end states of the CET are calculated in the radiological source term analysis. Since it is not practicable to perform source term analysis for each sequence of the CETs, the end states are grouped into Release Categories (RC). Source term analysis is then carried out for each Release Category. The source terms analysis defines the characteristics associated with each release, including the quantity of radioactive material, its isotopic composition, height and energy. This is necessary for the calculation of off-site doses under the Level 3 PSA.

The process of radiological source term analysis involves:

a) Specifying the RCs;

b) Grouping the end states of the CETs into the RCs;

c) Carrying out the source term analysis for the Release Categories using an appropriate code.

14.5.11.1 Specifying the RCs

The factors that influence fission product production, retention, and transport paths to the environment should be considered when defining the attributes of the release categories. The attributes chosen for the UK HPR1000 are listed as follows:

a) Containment bypass /no bypass

This is used to separate containment bypass sequences. Containment bypass sequences are listed as follows:

1) ISLOCA core damage sequences;

2) SGTR non-isolated core damage sequences.

b) Failure time of the containment

This is used to separate sequences associated with different containment failure times. The progress of a severe accident is separated into three stages which are listed as follows:

1) T1: the stage before RPV failure;

2) T2: the time of RPV failure;

3) T3: significant length of time after RPV failure.

c) Containment failure mode

The failure modes of the containment are listed as follows:

1) Containment isolation failure;

2) Containment rupture induced by severe accident phenomena;

3) Basemat melt through.

d) The pressure of the primary loop when RPV fails:

1) High pressure;

2) Low pressure.

e) Source terms mitigated by sprays or scrubbing (for bypass sequences):

1) With spray/ scrubbing;

2) Without spray/ scrubbing.

Sprays are considered for source term mitigation in all categories with containment failure. For bypass sequences (SGTR and ISLOCA) this characteristic represents whether or not the release is scrubbed by SG feed water. The proposed RCs listed in T-14.5-3 are presented in Reference [8].

T-14.5-3 Proposed RCs of UK HPR1000 Level 2 PSA

RCs	**Description**
RC101	Containment integrity
RC201	Containment isolation failure with containment spray
RC202	Containment isolation failure without containment spray
RC203	Early stage containment overpressure failure
RC301	T1 stage containment rupture before vessel failure due to hydrogen
RC303	T1 stage containment rupture before vessel failure due to steam explosion at low pressure
RC305	T1 stage containment rupture before vessel failure due to steam explosion at high pressure
RC401	T2 stage containment rupture due to vessel failure phenomena at low pressure
RC403	T2 stage containment rupture due to vessel failure phenomena at high pressure
RC501	T3 stage long term containment failure due to overpressure with containment sprays
RC502	T3 stage long term containment failure due to overpressure without containment sprays
RC503	T3 stage long term containment failure due to MCCI
RC601	SGTR without fission product scrubbing
RC602	SGTR with fission product scrubbing
RC701	ISLOCA
RC801	Large break in RPV

14.5.11.2 Grouping and Source Term Calculation

After RC classification is finished, each Level 2 PSA accident sequence is given an RC. Representative severe accident sequences with a conservative or bounding source term are chosen for each RC and the total activity of the fission products released from the containment is calculated. Each RC is represented by a single source term. The source terms represent the release to the environment for the different isotope groups considered in the model.

14.5.12 Main Results and Risk Insights

The results of the Level 2 PSA will include:

a) Larger Release Frequency (LRF)[1] and contributing RCs

b) RC frequency and the source terms

c) Uncertainty analysis of the LRF

d) Sensitivity analysis of the following aspects

    1) Phenomena

    2) Human errors

    3) Components

    4) Mission time

e) Importance analysis of the following aspects

    1) Phenomena

    2) Human errors

    3) Components

f) Source term analysis results

g) Risk insights

14.6 Spent Fuel Pool PSA

14.6.1 Introduction

The SFP PSA is used to quantitatively evaluate risks associated with the SFP and related fuel handling facilities, to identify the design shortfalls, and to give the corresponding risk insights.

Sub-chapter 14.6 covers Level 1 and Level 2 SFP PSAs. The methodology follows

[1] For the purpose of discussing “large release”, a qualitative criterion related to the failure modes of the containment are used. If one of the containment failure modes occurs, the release will be considered as large release.

Reference [33] and the key elements analysis refers to References [16], [17], [31] and [32].

14.6.2 Scope

The scope of the UK HPR1000 SFP PSA includes the SFP and fuel handling facilities in the NI (fuel handling in the reactor building). All the IEs (include internal events, and internal and external hazards) and all SFP operating states (including full power and LPSD states) are considered in the SFP PSA.

The SFP PSA is used to calculate the risk of Fuel Damage (FD) and radioactive substances release.

The SFP internal events Level 1 PSA is in Sub-chapter 14.6.5, the SFP internal and external hazards Level 1 PSA is in Sub-chapter 14.6.6, and the SFP Level 2 PSA is in Sub-chapter14.6.7.

14.6.3 Assumptions

The main assumptions of SFP PSA include:

a) In event of loss of SFP cooling and water inventory, FD is assumed once the top of fuel stored in SFP is uncovered.

b) It is assumed that the PTR [FPCTS] system cooling circuit is not available when the SFP water temperature is above 97°C.

c) When assessing the risk associated with the SFP caused by internal fire or internal flooding, it is assumed that all the components of interest in the SFP area are damaged.

d) The PTR [FPCTS] has three cooling trains (train A, train B and train C), and one cooling train (train A or train B) runs during the non-refuelling stage. In order to simplify the analysis, it is assumed that train A runs during the non-refuelling stage and the other two trains are available as backups.

e) It is assumed that water vapour generated by the SFP does not affect the normal operation of the surrounding equipment.

14.6.4 Methodology

Detailed descriptions of SFP PSA methodology for UK HPR1000 are in Reference [8] and Reference [9].

14.6.5 SFP Internal Events Level 1 PSA

Key elements adopted for the SFP PSA are as follows:

a) SFP operating states definition.

b) Initiating events analysis.

c) Accident sequence analysis.

d) System analysis.

e) Data analysis.

f) Human reliability analysis.

g) Quantification.

h) Results analysis and risk insights.

14.6.5.1 SFP Operating States Definition

The SFP PSA operating states are defined to represent various possible conditions during a refuelling cycle. Standard operating conditions form the basis of the SFP operating states definition, which are listed in Reference [19].

In order to facilitate the subsequent application of operating states to the SFP PSA, standard operating conditions are grouped based on the following factors:

a) Similarity of SFP status (e.g., decay heat of SFP).

b) Similarity of available systems and components (e.g., cooling types of SFP).

c) Similarity of IEs and plant responses.

14.6.5.2 Initiating Events Analysis

In the SFP PSA, an IE is an event that could lead directly to radioactive substance release or that challenges normal operation and which requires successful implementation of mitigation measures to prevent radioactive substance release from the SFP and fuel handling facilities in the nuclear island.

SFP PSA IE analysis includes:

a) Initiating events identification:

   1) Use of analytical methodology such as FMEA, and master logic diagrams to form an initial list of PIEs;

   2) Comparison between the list of PIEs developed with safety analysis and operating experience data for similar plants, to ensure the accuracy of the PIEs list.

b) Initiating events grouping

The IEs identified are grouped according to the similarity in plant responses, success criteria and allowable response time.

c) Initiating events frequency estimation

Each IE (group) frequency is derived from one of the following sources:

1) Data from generic site reports, Reference [24], such as the frequency of LOOP.

2) Data from the NUREG series, such as Reference [34].

3) The operating experience data from similar plants.

4) Data from FTA, such as loss of RRI [CCWS] or SEC [ESWS], and loss of PTR [FPCTS].

Detail methodology of SFP PSA IE analysis is included in Reference [3]. Following this, the categories below are considered in the internal event Level 1 SFP PSA.

a) Loss of SFP cooling;

b) Loss of SFP water inventory;

c) Fuel handling accident.

14.6.5.3 Accident Sequence Analysis

Accident sequence analysis is used to analyse the plant response to IEs and identify the sequences that may potentially lead to FD.

The methodology of accident sequence analysis for the SFP PSA is similar to that which is used for the internal events Level 1 PSA. This is described in Reference [2].

It is noted that there are some differences in the accident sequence analyses due to the different end states defined for the SFP PSA and internal events Level 1 PSA.

End states are used to identify the consequences of each accident sequence. SFP PSA accident sequence end states are defined as OK or FD.

OK and FD are defined as follows:

a) OK: no damage to fuel.

b) FD: fuel damage, which is divided into two categories:

    1) Thermal damage: refers to fuel exposed and damaged due to loss of cooling systems or loss of water inventory in the SFP or reactor pool.

    2) Mechanical damage: refers to fuel damaged caused by an external force resulting in the release of radiological materials, such as FD following a fuel handling accident.

14.6.5.4 System Analysis

System analysis aims to assess the paths and probabilities of failure of the systems required to mitigate accidents.

The SFP PSA system analysis methodology is similar to the internal events Level 1

PSA methodology described in Reference [2].

The systems that need to be analysed include:

a) PTR [FPCTS] and its support systems (e.g., RRI [CCWS]/ SEC [ESWS] and power supply systems);

b) I&C signal related systems;

c) SFP cooling water supply systems (e.g., Secondary Passive Heat Removal System (ASP [SPHRS])).

14.6.5.5 Human Reliability Analysis

HRA aims to ensure that the impacts of human error are reflected in the SFP PSA. Three types (type A, type B, type C) of human error events are considered in the SFP PSA, which are introduced in Reference [4].

It is noted that there is a large water inventory in the SFP, and, in event of loss of SFP cooling and water inventory, the time window for human action is sufficiently long to enable remedial actions to be implemented over the course of several operator shifts. After an IE occurs, if the existing shift cannot mitigate the accident, the subsequent shift can take charge. Therefore, the possibility of recovery after the failure of human actions can still be considered if the time window for operation is sufficient.

14.6.5.6 Data Analysis

Data analysis aims to provide all data required for quantification of the model. The data include:

a) Equipment failure probability.

b) Unavailability caused by equipment test and maintenance.

c) CCF parameter.

Methodology and analysis processes used for SFP PSA data analysis are consistent with the internal events Level 1 PSA, Reference [12].

14.6.5.7 Quantification

Quantification calculates the Fuel Damage Frequency (FDF) of each accident sequence and the total FDF, and identifies minimal cut-sets of accident sequences and the dominant accident sequences leading to FD. Sensitivity analysis, importance analysis and uncertainty analysis are undertaken as part of this.

Methodology and analysis processes are consistent with the internal events Level 1 PSA, Reference [2].

14.6.5.8 Main Results and Risk Insights

This section provides a summary of SFP PSA results for internal IEs. The results and insights will include:

a) Total FDF;

b) Contribution to FDF by various groups of IEs;

c) Contribution of different POSs;

d) Dominant fuel damage sequences;

e) Minimal cut-set analysis results;

f) Sensitivity analysis results;

g) Uncertainty analysis results;

h) Risk insights.

14.6.6 SFP Internal and External Hazards Level 1 PSA

The SFP internal and external hazards Level 1 PSA is used to assess the risk associated with the SFP and fuel handling facilities in the nuclear island due to internal and external hazards. In the SFP PSA, screened-in internal and external hazards in Reference [11] are as follows:

a) Internal hazards

  1) Internal fire;

  2) Internal flooding;

  3) Dropped load.

b) External hazards

  1) Strong wind;

  2) Tornado;

  3) Extreme snow (including snowstorm);

  4) Seismic hazards;

  5) Frazil ice;

  6) Ice barriers;

  7) External flooding;

  8) Organic material in water;

  9) Strong wind and organic material in water;

10) Strong wind and extreme snow;

11) Seismic hazards induced internal fire or flooding.

The analysis process and methodology for the internal and external hazards Level 1 SFP PSA is similar to that which is used for the reactor core Level 1 PSA. The internal and external hazards SFP Level 1 PSA will be described in SFP Level 1 PSA report.

14.6.7 SFP Level 2 PSA

The SFP Level 2 PSA uses analysis results from the SFP Level 1 PSA as the analysis starting point, it considers the effectiveness of the measures for the retention of radioactive substances in the power plant after FD, and conducts corresponding source analyses, so that it evaluates the risk of radioactive substance release from the SFP and fuel handling facilities in the NI.

The analysis process and methodology of the Level 2 SFP PSA are similar to Level 2 PSA for the reactor core, and this work will be completed and described in Level 2 PSA report.

14.7 Additional Sources of Radioactivity Risk Assessment

The sources of radioactivity assessment are used to estimate whether the risk induced by those sources challenges radiation protection targets 5~9.

Other sources of radioactivity include waste storage tanks from multiple systems (including Coolant Storage and Treatment System (TEP [CSTS]), Liquid Waste Treatment System (TEU [LWTS]), etc.).

The details of radiation protection targets 5~9 are described in Sub-chapter14.9.

14.8 Level 3 PSA

14.8.1 Introduction

The objective of the Level 3 PSA is to analyse off-site consequences caused by accidents on the UK HPR1000 site leading to risks to the public. In addition, Level 3 PSA forms an important part of GDA, and is a tool to assess whether the radiological risks are controlled and reduced ALARP. This section describes the scope and the methodology of the Level 3 PSA to be applied to the UK HPR1000.

14.8.2 Scope

Level 3 PSA presents the consequences of Level 2 and non-core damage in Level 1 radionuclide release at a nuclear facility. It is concerned with the analysis of the release of radionuclides and their transfer through the environment, and with risks to the public from off-site releases. These consequences may be stochastic health effects or deterministic health effects in nature. Stochastic health effects are the likelihood of long term health consequences to those affected by the radionuclide release. Deterministic health effects are the estimated immediate health effects (i.e. fatalities and injuries) as a result of the radionuclide release. The scope of the Level 3 PSA is to assess the following individual risk and the societal risk during the GDA phase according to off-site radiation protection targets and overall radiation protection target for fault and accident conditions in Reference [35] which are equivalent to the Numerical Targets 7, 8 and 9 set out in Reference [36]. These radiation protection targets are presented in Sub-chapter 14.9.2 and Sub-chapter 14.9.3.

14.8.3 Methodology

The UK HPR1000 Level 3 PSA will be based on Reference [37].

The UK HPR1000 Level 3 PSA demonstrates that the off-site and overall radiation protection targets are met with the risk not exceeding the Basic Safety Level (BSL), and assists with demonstrating that risks are ALARP.

This section presents the methodology and the Level 3 PSA process.

14.8.3.1 Identification of Potential Radiological Release Fault Sequences for Assessment

In order to estimate the individual risk to persons off-site from accidents on site, the comprehensive potential radiological release fault sequences are first identified. Level 1 and Level 2 PSAs (as described in Sub-chapters 14.4, 14.5 and 14.6) provide inputs for the Level 3 PSA.

A comprehensive Level 1 PSA is performed encompassing all IEs (internal events, and internal and external hazards), all POSs, and all sources of radioactivity at the facility included in the plant (reactor core, SFP, radioactive wastes and new fuel).

The Level 2 PSA outputs are key inputs to the Level 3 PSA, i.e. the RCs, which are groups of accident sequences. Each RC chooses a representative accident sequence from which the associated source term is derived.

There are low dose bands for off-site radiation protection targets, which are equivalent to Numerical Target 8. This means the non-core damage radionuclide release should be considered as a part of the inputs.

The Level 1 PSA "success" sequences which result in radiological material release to the environment from the facility are also included as inputs for the UK HPR1000 Level 3 PSA. The success sequences are first identified and grouped according accident characteristics. The Level 1 PSA success sequences are assigned to an RC with associated source term information.

For each RC, the source term and potential radiological release characteristics are provided, including:

a) Quantity of radioactivity.

b) Isotopic composition.

c) Chemical composition.

d) Particle size distribution.

e) Duration of release.

f) Rate of energy release.

g) Height of release.

h) Building dimensions, i.e. building wake effects.

i) Frequency of the identified accident.

The characteristics of these releases are usually grouped by their similar features. The combined characteristics of a release are referred to as a source term.

14.8.3.2 Calculation of Individual Dose and Corresponding Frequency Combining with Generic Site Parameters

To estimate the dose to individuals off-site, the Level 3 PSA requires the source term information, meteorology, the assumed location of the individual off site and protective actions. There are several principal exposure pathways through which people can accumulate a radiation dose after accidental radionuclide release to the atmosphere. The dose calculation also contains the age group, the rate of inhalation, the dose conversion factors, and the duration of exposure. The individual dose calculated is coupled with the frequency of the accident for comparison to targets. Best-estimate methods and data are used for the choice of relevant parameters, models and methodology.

a) The transportation of radionuclides nuclides in the environment

The plume created by the released radionuclides as fine aerosol or gas expands horizontally and vertically owing to diffusion and turbulent eddies in the atmosphere. The plume dispersion is only the starting point for the model of how released plumes behave in the atmosphere. There are several other phenomena to be considered, including the atmospheric dispersion and deposition model, for instance, buoyant plume rise, building wake effects, wet deposition (due to rain), dry deposition, resuspension, radiological decay, etc. These factors could increase or reduce the quantities of radionuclides from or in the plume as they spread across the region.

The typical characterisations of meteorology are provided as a data file containing wind speed, wind direction, stability category, rainfall and mixing layer depth. However, during the GDA phase, a “generic site” is the assessment object of the Level 3 PSA. The choice and decision on “generic site” fits the UK context, and is specified carefully and conservatively. The calculation is developed based on site-specific characteristics during the nuclear site licensing phase.

b) Exposure pathways

The radiological consequence to a person off-site is dependent on a number of different exposure pathways through which dose can be received following an accidental radionuclide release to the atmosphere. The external pathways contain cloud shine, ground shine and deposition onto skin. And the internal pathways contain direct inhalation, resuspension inhalation and ingestion from food and water.

Early exposure considers the following pathways:

1) The external irradiation from radionuclides in the passing plume.

2) The external irradiation from radionuclides deposited on the ground.

3) The external irradiation from radionuclides deposited on the skin and clothing.

4) The internal irradiation from inhalation of radionuclides in the passing plume.

5) The internal irradiation from resuspended radionuclides.

The intermediate and long-term exposure considers the following pathways:

1) The external irradiation from radionuclides deposited on the ground.

2) The internal irradiation from resuspended radionuclides.

3) The internal irradiation from inhalation and ingestion of contaminated food and water.

Dose conversion factors respective to each exposure pathway are drawn from sources such as International Commission on Radiological Protection recommendations.

c) Health effects

There are two main types of health effects on the people exposed to ionising radiation. One type is the deterministic effects caused by high dose exposure. This may be observed as functional loss of tissues or organs, and even the acute death. There is usually a dose threshold. Another is stochastic effects which increase the incidence of cancer and hereditary disease, and may cause eventual death. There is no dose threshold, but the incidence is proportional to the dose (the linear no threshold model).

d) Justified countermeasures

Generally, there are two categories of protective actions which may be taken after or during the accidental radionuclide release to reduce the influence of the accident on the public. One category is called short-term protective actions which usually include sheltering, evacuation, the issuing of stable iodine tables, and decontamination. Another is long-term protective actions which include relocation, land and building decontamination and food bans.

e) Other important parameters

1) Assumed location of the hypothetical person

During the generic assessment, without site-specific knowledge of the habitation locations or likely occupancy, a range of hypothetical person locations are assessed to determine the point of greatest dose. The range includes assessment at the minimum distance between the facility and the site boundary, as defined with reference to the generic plant.

Besides the location of the individual, the age group is also taken into account.

2) Agricultural production data, land data and food distribution data

Agricultural production data, land data and food distribution data are used to calculate the dose to the off-site people in accident conditions.

14.8.3.3 Comparison with Off-site Radiation Protection Targets

Targets for the risk of death to an individual off-site are used in conjunction with the targets for the total predicted frequencies for accidents, which could result in a person off site receiving a radiological dose. This is site specific, and a dose-frequency staircase is derived for the off-site individual risk of death. Comparison against the BSLs for dose-frequency targets will be to be demonstrated, and the risk will be reduced ALARP.

After the identification of fault sequences and estimation of consequence, each fault sequence is assigned to its corresponding dose band, as illustrated by the dose-frequency targets, based on the estimated dose of each. The total frequency for scenarios in each dose band is compared against the BSLs and Basic Safety Objectives (BSOs), and the argument for demonstration of ALARP is developed.

14.8.3.4 Comparison with Overall Radiation Protection Target

Overall radiation protection targets are used in the assessment of societal risk following a severe accident or non-core damage radionuclide release from the facility.

The countermeasures would be taken in to account according RGPs and UK context for the radiation emergency.

There are notable differences between the risk to an individual off-site and the societal risk. The screening rules are provided and applied to identify the accident sequence which may cause 100 or more fatalities in the wider population, either immediate or eventual, from exposure to radiation.

The summated frequency of the identified accident sequences which lead to 100 or more fatalities, either immediate or eventual, from radiological exposure, are compared against overall radiation protection target.

14.8.4 Main Results and Risk Insights

Sensitivity and uncertainty analysis for Level 3 PSA will be performed to demonstrate that the results of the Level 3 assessment and associated conclusions are not compromised. The Level 3 PSA supports judgment made about the overall acceptability of the design through demonstrating compliance with off-site radiation protection targets and the overall radiation protection target (Numerical Targets 7, 8 and 9). It also will demonstrate that the significant contributors to the risk are understood and analysed as a part of the overall UK HPR1000 ALARP process (see Sub-chapter 14.10).

14.9 Radiation Protection Targets Evaluation

14.9.1 Radiation Protection Targets 5 and 6 Evaluation

This sub-chapter outlines the requirement and preliminary assessment of potential radiological risk to a worker on site against the on-site radiation protection targets as defined in Reference [35] (equivalent to the Numerical Targets 5 and 6 set out in Reference [36]).

The on-site radiation protection targets for faults and accidents conditions require:

a) Assessment of the summated individual risk of death from faults/accidents for any person on the site (Numerical Target 5).

b) Assessment for each single fault against frequency/worker dose targets (Numerical Target 6).

The demonstrations of radiation protection targets 5 and 6 are based on the PSA and other preliminary assumptions regarding worker dose and risk evaluation. The worker risk assessment in this sub-chapter is limited to the potential radiological risk to workers on site due to accident conditions. Conventional risk will not be included in the assessment. The potential radiological risk due to medium and long-term post-accident activities once a safe state has been reached, such as material/fuel recovery and clean-up operations, is outside the scope of GDA.

The fault considered in the worker risk assessment includes:

a) All IEs considered in the UK HPR1000 PSA.

b) Representative fault groups generated from the success sequences in the Level 1 PSA.

c) Release Categories generated from the Level 2 PSA.

d) Any other fault that requires direct intervention of workers for mitigation.

Worker dose assessments are performed for each accident sequence for any person on the site. The maximum dose received by workers will be calculated based on the following inputs:

a) The location of the worker.

b) The duration of the exposure.

c) The source term of the contained and uncontained source.

14.9.2 Off-site Radiation Protection Targets Evaluation

This sub-chapter outlines the requirements for reducing the potential radiological risk to an off-site individual against off-site radiation protection targets.

a) The targets for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation, are:

BSL: 1×10^{-4} pa;

BSO: 1×10^{-6} pa.

b) The targets for the total predicted frequencies of accidents on an individual facility, which gives doses to an off-site person, are as presented in T-14.9-1.

T-14.9-1 Frequency Dose Targets for Accidents on an Individual Facility – Any Person off the Site

Effective dose (mSv)	**Total predicted frequency per annum**	
	BSL (pa)	**BSO (pa)**
0.1~1	1	1×10^{-2}
1~10	1×10^{-1}	1×10^{-3}
10~100	1×10^{-2}	1×10^{-4}
100~1000	1×10^{-3}	1×10^{-5}
>1000	1×10^{-4}	1×10^{-6}

These targets are equivalent to the Numerical Targets 7 and 8 set out in Reference [36]. Further information on the assessment methodology is presented in Sub-chapter 14.8.

Demonstration of compliance with off-site radiation protection targets will be provided in Level 3 PSA report.

14.9.3 Overall Radiation Protection Target Evaluation

The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation, are:

BSL: 1×10^{-5} pa;

BSO: 1×10^{-7} pa.

These targets are equivalent to those given in Numerical Target 9 set out in Reference [36]. Further information on the assessment methodology is presented in Sub-chapter 14.8.

Overall radiation protection target demonstration will be provided in Level 3 PSA report.

14.10 Overall PSA Insights and ALARP Assessment

14.10.1 Overall PSA Insights

The PSA provides important insight into the design and supports decision-making. PSA results are used to assess the level of safety and identify shortfalls in the design.

a) Accidents sequence results are used to identify the dominant fault sequences and events contributing to risk. The contributions to the overall risk from different IEs are used to determine whether the design of the plant is balanced so that no particular group of IEs and no particular accident sequence make an unduly large contribution to the overall risk. If possible, improvements are supplied for decision-making to gain the balanced design.

b) The dominant minimal cut-sets are used to identify where there are relative weaknesses in the design stage and determine whether there are any single order minimal cut-sets that indicate that the single failure requirement is not complied with any safety systems. If possible, improvements are supplied to increase the diversification of diversiform equipment and system for decision-making to meet the single failure criterion.

c) Risk importance analysis can identify more significant contribution to the risk results, such as FV and RIF. Importance measures for basic events, IEs, etc., can be calculated and used to interpret the results of the PSA. The importance values are used to identify the components and systems that significantly contribute to the risk and are considered carefully at the design level. The importance values are used to identify areas of the design where improvements might be considered.

    1) A high FV importance value for an independent failure event may indicate insufficient redundancy of the system in some plant operating states. If so, either the system's redundancy might be increased or limiting conditions for

operation of the system might be made more rigorous for the particular plant operating mode, if possible. A high RIF for an independent failure event may indicate that the level of reliability of the equipment might be carefully maintained to avoid an increase in risk.

2) A high FV importance value for a CCF may indicate insufficient diversity of safety systems in respect of a particular safety function. If possible, improvements are supplied to increase the diversification of equipment and system for decision-making.

d) Sensitivity analysis and uncertainty analysis can help ensure that important uncertainties are understood and reduced where possible.

14.10.1.1 PSA Used in HPR1000 Design Development

In the process of HPR1000 design development, PSA has been used to support technical decision-making, and these cases are described as follows:

a) Technical solution of safety system configuration

In the initial stage of HPR1000 research and development, several technical solutions of safety system configuration were proposed, which were based on the design and construction engineering experience of ACPR1000 along with the technical and performance requirements of the third generation advanced reactors (such as EUR&URD), combined with current industrial development level. PSA was used to evaluate the different technical solutions for the safety system configuration, and to eventually give the evaluation conclusions and recommendations to support the selection of technical solutions.

b) Evaluation of system design improvement

During the HPR1000 design stage, several system design optimisation recommendations were proposed to improve the safety or economy of the NPP while balancing the two at the same time. The PSA provided analysis and evaluation for each system design improvement, and gave the conclusions and suggestions to support technical decision-making.

c) Identification of Design Extension Condition A (DEC-A)

During the design of DEC-A condition list for the HPR1000, accident sequence frequency in PSA was considered as an important screening criteria to identify the DEC-A condition and the additional safety characteristics (DEC-A characteristics) were defined to prevent the occurrence of severe accidents following a DEC-A condition.

d) Selection of severe accident sequences

In the process of selecting severe accident sequences of HPR1000, PSA provided the sequence of dominant accidents that could cause core damage, which is an important input for the selection of severe accident sequences.

14.10.1.2 PSA Used in UK HPR1000 Design

The PSA provides important risk insights for the UK HPR1000 design and supports decision-making during the UK HPR1000 GDA phase. These outputs from the PSA will be used to identify aspects of the plant where potential design improvements can help reduce the overall plant risk. This includes:

a) UK HPR1000 balanced design evaluation

In the UK HPR1000 design process, with the PSA being developed according to acknowledged international good practice, the contributions to the overall risk from the dominant accident sequences and the dominant minimum cut sets from the PSA results will be used to determine whether the design of the UK HPR1000 is balanced so that no particular group of IEs and no particular accident sequence make an unduly large contribution to the overall risk. If possible, improvements will be supplied for decision-making to gain the balanced design.

PSA recommendations will be proposed as one of the inputs for UK HPR1000 design modification. After the design modification is complete, PSA evaluation is carried out again to form a closed-cycle in order to ensure that the plant design is well balanced.

b) Design improvements evaluation

The design improvements for the UK HPR1000 will be evaluated using PSA, and this evaluation will be carried out during the entire process of design improvement. In the proposal stage of design improvement, the PSA will used to preliminarily evaluate and judge the necessity of the design improvement.

In the design improvement implementation phase, PSA will also be used to provide support for the design scheme comparison and selection. After the design improvement is completed, PSA will also be carried out to provide the final comprehensive assessment on nuclear safety in order to ensure that the design improvements have achieved the intended objectives. In this process, the design improvements proposed will be managed to comprehensively evaluate the influence of the design modifications on key factors such as layout design, system design, nuclear safety and economy, etc. The PSA is just one aspect of the influence assessments on nuclear safety.

c) Radiation Protection Targets evaluation

During the UK HPR1000 GDA phase, PSA will be used to demonstrate whether the UK HPR1000 meets radiation protection targets 5 to 9. As part of this process, PSA will provides detailed quantitative analysis based on the UK HPR1000 PSA models to obtain the radiological release sequence and frequency for the demonstration of radiation protection targets. Radiation protection targets evaluation is described in Sub-chapter 14.9.

d) ALARP assessment

During the design of the UK HPR1000, PSA will be used to support the demonstration of ALARP in Reference [38]. This demonstration gives an introduction on the evolution of the UK HPR1000 design, and reviews the design improvements that have made significant contributions to design safety. The PSA analysis will be used to demonstrate that the evolution of UK HPR1000 is continuously reducing risk and optimising design toward ALARP. The ALARP assessment is described in Sub-chapter 14.10.

14.10.2 ALARP Assessment

As part of the overall UK HPR1000 ALARP process (PCSR Chapter 33), a comprehensive ALARP assessment in Chapter 14 PSA is performed according to the ALARP methodology provided in Sub-chapter 33.4 and Reference [38]. The ALARP assessment of Chapter 14 PSA includes two parts, as follows:

a) The process of PSA is ALARP. It is described in Sub-chapter14.10.2.1.

b) PSA provides risk insights and will be used in UK HPR1000 ALARP demonstration. It is described in Sub-chapter14.10.2.2.

14.10.2.1 ALARP Demonstration of the PSA Process

Relevant Good Practice identification

RGP identification is the starting point of ALARP analysis. A good review of RGP is undertaken to identify suitable options to reduce the risk.

The RGP and international practices applicable to PSA modelling are recognised in Sub-chapter 14.3. In PSA modelling, ONR expectations, Regulatory Query (RQs) of UK HPR1000 and other GDA projects, experience and feedback from other PSA projects are also considered.

Consistency Analysis against RGP and International Good Practices

The consistency analysis is carried out based on the requirements from RGP and international good practices. The result shows that no significant gaps are identified in methodologies of PSA. PSA models and reports will be created to justify that the PSA models are ALARP.

The consistency analysis against RGP and international good practice is a continuous process during the GDA phase, and PSA models and reports will be updated continuously according to the results of consistency analysis.

14.10.2.2 PSA Risk Insights Used in ALARP Demonstration

As part of the overall UK HPR1000 ALARP process (PCSR Chapter 33), the insights from PSA are managed appropriately to inform the priorities for risk improvement, evaluate improvements appropriately (for example, through an optioneering process) and determine whether the implementation of improvements is reasonably practicable.

The PSA will be updated at the different stages of the GDA process to reflect design changes accurately and demonstrate the improvements in overall plant risk.

The PSA will analyse the UK HPR1000 design and identifies further opportunities for risk reduction, through undertaking the following steps in GDA step 3 and step 4:

a) Demonstration that the UK HPR1000 meets radiation protection targets 5 to 9 following a systematic and comprehensive analysis of risk undertaken through PSA.

b) Identification of improvements to risk where previous stages of the PSA development has influenced the design.

c) Identified sequences and plant features that are shown to contribute to the risk are further considered, with potential opportunities for design changes identified and assessed. This evaluation forms part of the UK HPR1000 ALARP process (Chapter 33) and involves ALARP reviews/optioneering studies to ensure that all relevant considerations are taken into account and practicable steps are taken to reduce risks.

d) Outcomes from ALARP reviews will be incorporated into the PSA and presented during various steps of GDA phase (and beyond).

14.11 Concluding Remarks

The UK HPR1000 PSA is a full-scope PSA that includes assessment of all sources of radioactivity present at the facility, all types of IEs and covers all plant operating states and Level 1, Level 2 and Level 3 PSA.

The UK HPR1000 PSA is developed in accordance with methodology that is consistent with international standards.

PSA as a tool has been used to inform design process, and is used throughout the GDA phase for development of the UK HPR1000.

The risk estimation generated by the HPR1000 (FCG3) PSA results provides confidence that the PSA developed for the UK HPR1000 is able to demonstrate compliance with the radiation protection targets defined in Reference [35] and demonstrate that risks are ALARP. The areas that require enhancement for developing the UK HPR1000 PSA are identified and incorporated.

14.12 References

[1] CGN, UK HPR1000 Design Reference Report, Rev C, 2018.

[2] CGN, Methodology of Internal Event Level 1 PSA, GHX00650027DOZJ02GN, Rev A, 2018.

[3] CGN, Methodology of PIE Identification, GHX00100008DOZJ03GN, Rev F, 2018.

[4] CGN, Methodology of Human Reliability Analysis, GHX00650030DOZJ02GN, Rev A, 2018.

[5] CGN, Methodology of Internal Fire PSA, GHX00650033DOZJ02GN, Rev A, 2018.

[6] CGN, Methodology of Internal Flooding PSA, GHX00650031DOZJ02GN, Rev A, 2018.

[7] CGN, Methodology of External Hazards PSA, GHX00650032DOZJ02GN, Rev A, 2018.

[8] CGN, Methodology of Level 2 PSA, GHX00650028DOZJ02GN, Rev A, 2018.

[9] CGN, Methodology of Spent Fuel Pool PSA, GHX00650029DOZJ02GN, Rev A, 2018.

[10] CGN, Initiating Events List of Internal Event Level 1 PSA, GHX00650016DOZJ02GN, Rev D, 2018.

[11] CGN, The Identification and Screening of Internal and External Hazards in PSA, GHX00650034DOZJ02GN, Rev A, 2018.

[12] CGN, Data Analysis Report, GHX00650015DOZJ02GN, Rev C, 2017.

[13] NRC, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928, 2015.

[14] NRC, Common-Cause Failure Parameter Estimations, NUREG/CR-5497, 2015.

[15] CGN, General Principles for Application of Laws, Regulations, Codes and Standards, GHX00100018DOZJ03GN, Rev F, 2018.

[16] IAEA, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-3, IAEA, Vienna 2010.

[17] ASME, Addenda to ASME/ANS RA-S 2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant

Applications, ASME/ANS RA-Sb–2013, 2013.

[18] IAEA, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA-TECDOC-1804, 2016.

[19] CGN, Definition of Normal Operating Modes and Corresponding Parameters, GHX71100001DOYX03GN, Rev B, 2018.

[20] NRC, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, 1996.

[21] NRC, Handbook of Human Reliability analysis with Emphasis on Nuclear Power Plant Application Final Report, NUREG/CR-1278, 1883.

[22] NRC, The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883, 2005.

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

[24] GNS, UK HPR1000 Generic Site Report, HPR/GDA/REPO/0015, Rev V0, 2017.

[25] EPRI/NRC-RES, Fire PRA methodology for nuclear power facilities, Final Report, NUREG/CR-6850, EPRI 1011989, 2005.

[26] NRC, Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database, NUREG-2169, 2009.

[27] EPRI, Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment, Electric Power Research Institute, EPRI 1019194, 2009.

[28] EPRI, Seismic Probabilistic Risk Assessment Implementation Guide, EPRI TR-3002000709, 2013.

[29] EPRI, A Methodology for Assessment of Nuclear Power Plant Seismic Margin (Revision 1), EPRI NP-6041-SL, 1991.

[30] EPRI, Methodology for Developing Seismic Fragilities, EPRI TR-103959, 1994.

[31] IAEA, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety guide No. SSG-4. IAEA, Vienna 2010.

[32] ASME, Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs), ASME/ANS RA-S-1.2-2014, 2014.

[33] EPRI, PWR Spent Fuel Pool Risk Assessment Integration Framework and Pilot Plant Application, EPRI-3002002691, 2014.

[34] NRC, Operating Experience Feedback Reports, NUREG -1275, 1997.

[35] CGN, General Safety Requirements, GHX00100017DOZJ03GN, Rev C, 2018.

[36] ONR, Safety Assessment Principles for Nuclear Facilities. 2014 Edition, Revision 0.

[37] ASME, Standard for Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications, ASME/ANS RA-S-1.3-2017, 2017.

[38] CGN, ALARP Methodology, GHX00100051DOZJ03GN, Rev B, 2018.