Revision	Approved by	Number of Pages
001		222
Approval Date	06/02-20	

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	HPR/GDA/PCSR/0013

Title:

Pre-Construction Safety Report

Chapter 13

Design Extension Conditions and Severe Accident Analysis

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

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

Text within this document that is enclosed within brackets '{...}' contains Sensitive Information and has been removed.

DISTRIBUTION LIST

Recipients	Cross Box
General Nuclear System Executive	☐
General Nuclear System all staff	☐
General Nuclear System and BRB all staff	☒
CGN	☒
EDF	☒
Regulators	☒
Public	☒

TABLE OF CONTENTS

13.1 List of Abbreviations and Acronyms

AAD	Startup and Shutdown Feedwater System [SSFS]
AC	Alternating Current
ACC	Accumulator
ALARP	As Low As Reasonably Practicable
APG	Steam Generator Blowdown System [SGBS]
ARE	Main Feedwater Flow Control System [MFFCS]
ASG	Emergency Feedwater System [EFWS]
ASP	Secondary Passive Heat Removal System [SPHRS]
ATWS	Anticipated Transient Without Scram
CAE	Claims - Arguments - Evidence
CCF	Common Cause Failure
CDF	Core Damage Frequency
CET	Containment Event Tree
CFD	Computational Fluid Dynamics
CGN	China General Nuclear Power Corporation
CHF	Critical Heat Flux
CRF	Circulating Water System [CWS]
DBC	Design Basis Condition
DCH	Direct Containment Heating
DDT	Deflagration to Detonation Transition

DEC	Design Extension Condition
DEL	Safety Chilled Water System [SCWS]
DG	Diesel Generator
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DR	Design Reference
DWL	Safeguard Building Controlled Area Ventilation System [SBCAVS]
ECS	Extra Cooling System [ECS]
EDE	Annulus Ventilation System [AVS]
EDG	Emergency Diesel Generator
EHR	Containment Heat Removal System [CHRS]
EOL	End Of Life
EOP	Emergency Operating Procedure
EPP	Containment Leak Rate Testing and Monitoring System [CLRTMS]
EUF	Containment Filtration and Exhaust System [CFES]
EUH	Containment Combustible Gas Control System [CCGCS]
FCI	Fuel Coolant Interaction
FP	Full Power
GCT	Turbine Bypass System [TBS]
GDA	Generic Design Assessment

HF	Human Factors
HIC	High Integrity Components
HIRE	Hazard Identification and Risk Evaluation
HPME	High Pressure Melt Ejection
HPR1000 (FCG3)	Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IB-LOCA	Intermediate Break - Loss of Coolant Accident
IRWST	In-containment Refuelling Water Storage Tank
ISLOCA	Interfacing Systems Loss of Coolant Accident
ISP	International Standard Problems
IVR	In-Vessel Retention
KDS	Diverse Actuation System [DAS]
KIT	Karlsruhe Institute of Technology
KRT	Plant Radiation Monitoring System [PRMS]
LB-LOCA	Large Break - Loss of Coolant Accident
LCD	Low Pressure Full Cooldown
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOMFW	Loss of Main Feedwater

LOOP	Loss of Offsite Power
LUHS	Loss of Ultimate Heat Sink
MASCA	MATERIAL SCALING
MCCI	Molten Core-Concrete Interaction
MCD	Medium Pressure Rapid Cooldown
MCR	Main Control Room
MCS	Maintenance Cold Shutdown
MHSI	Medium Head Safety Injection
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSSV	Main Steam Safety Valve
NNSA	National Nuclear Safety Administration
NPP	Nuclear Power Plant
NR	Narrow Range
NS/SG	Normal Shutdown with Steam Generators
OECD	Organization for Economic and Cooperation Development
ONR	Office for Nuclear Regulation
PAR	Passive Autocatalytic Recombiner
PCSR	Pre-Construction Safety Report
PCT	Peaking Cladding Temperature
PDF	Probability Distribution Function

PIE	Postulated Initiating Events
POS	Plant Operating State
PSA	Probabilistic Safety Assessment
PSV	Pressuriser Safety Valve
PTR	Fuel Pool Cooling and Treatment System [FPCTS]
PWR	Pressurised Water Reactor
PZR	Pressuriser
RBS	Emergency Boration System [EBS]
RC	Release Category
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant System [RCS]
RCPB	Reactor Coolant Pressure Boundary
RCV	Chemical and Volume Control System [CVCS]
REA	Reactor Boron and Water Makeup System [RBWMS]
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RIS	Safety Injection System [SIS]
RMI	Reflective Metallic Insulations
ROAAM	Risk Oriented Accident Analysis Methodology
RPS	Protection System [PS]
RPT	Radiation Protection Target

RPV	Reactor Pressure Vessel
RRI	Component Cooling Water System [CCWS]
RT	Reactor Trip
SA	Severe Accident
SAA	Severe Accident Analysis
SAMG	Severe Accident Management Guideline
SADV	Severe Accident Dedicated Valve
SAPs	Safety Assessment Principles for Nuclear Facilities
SARNET	Severe Accident Research Network of excellence
SB-LOCA	Small Break - Loss of Coolant Accident
SBO	Station Black Out
SEC	Essential Service Water System [ESWS]
SED	NI Demineralised Water Distribution System [DWDS (NI)]
SFP	Spent Fuel Pool
SERG	Steam Explosion Review Group
SG	Steam Generator
SGa	Affected Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SLB	Steam Line Break
SSC	Structures, Systems and Components

TAG	Technical Assessment Guide
TLOCC	Total Loss of Cooling Chain
TLOFW	Total Loss of Feedwater
TSC	Technical Support Centre
TSP	Tri-Sodium Phosphate
UHS	Ultimate Heat Sink
UK HPR1000	UK version of the Hua-long Pressurised Reactor
UPS	Uninterruptible Power Supply
VDA	Atmospheric Steam Dump System [ASDS]
VVP	Main Steam System [MSS]
WENRA	Western European Nuclear Regulators' Association
WR	Wide Range

System codes (XXX) and system abbreviations (YYY) are provided for completeness in the format (XXX [YYY]), e.g. Emergency Feedwater System (ASG [EFWS]).

13.2 Introduction

The analysis of Design Basis Condition (DBC) events is described in Chapter 12. The purpose of the Design Basis Analysis is to demonstrate that the design can respond to any fault with an initiating event frequency > 1E-5 per reactor year and achieve a safe state with a tolerable level of radiation exposure or release of radioactive material. However, additional protection and mitigation measures are included in the design to respond to failures in the design basis safety systems or to initiating events beyond the design basis; these are termed Design Extension Conditions (DEC).

DEC events are low frequency sequences where the conditions may be more severe than those identified in the DBC analysis. DEC events are placed into two classes, which are assessed using different methodologies due to the different phenomena encountered as discussed below:

DEC-A: These are complex sequences which involve failures beyond those

considered in the design basis analysis or sequences following more severe initiating events than those considered in the design basis analysis; however, the additional DEC-A protection measures are successful in preventing core damage. Therefore, the sequences are derived on the basis of engineering judgement, DBA and Probabilistic Safety Assessment (PSA).

DEC-B: These are sequences in which the protection systems designed to prevent core or spent fuel damage fail and core or spent fuel damage does occur. Despite core melting, significant radiological impacts can be avoided if an intact containment can be maintained; this is achieved by including severe accident mitigation measures in the design to prevent or control accident progression. The sequences used for the severe accident mitigation measure effectiveness assessment are identified from the PSA and deterministic analysis combined with engineering judgment.

The present safety case of DEC-A and Severe Accident Analysis is produced based on the Design Reference (DR) version 2.0, as described in the UK HPR1000 Design Reference Report (Reference [1], Rev.D). The safety assessment results are documented in this chapter and corresponding reports. However, all the design changes between DR2.0 and DR2.1 have been assessed from DEC-A and Severe Accident Analysis point of view and corresponding insights have been provided to support the determination of these design changes.

13.2.1 Chapter Route Map

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

To underpin this objective, five high level claims and a number of level 2 claims are developed and presented in Chapter 1. The main objective of this chapter is to present the analysis of DECs in the UK HPR1000. This chapter supports ***Claim 3.2*** and ***Claim 3.4*** derived from the high level ***Claim 3***.

Claim 3*: The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defence to fulfil the fundamental safety functions, reducing the nuclear safety risks to a level that is As Low As Reasonably Practicable (ALARP).*

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

Claim 3.2.3*: Analysis of Design Extension Conditions and Severe Accident Analysis have been carried out to identify further risk reducing measures..*

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

***Claim 3.4.7**: Analysis of Design Extension Conditions including Severe Accident Analysis demonstrates further defence in depth, identifying additional accident prevention or mitigating measures and emergency arrangements.*

To support *Claim 3.2.3* and *Claim 3.4.7*, this chapter develops several Sub-claims and a number of relevant arguments and evidence:

The following key information will be presented in this chapter through all Generic Design Assessment (GDA) steps:

a) ***Sub-Claim 3.2.3.SC13.1: There is no cliff-edge beyond DBC.***

1) ***Argument 3.2.3.SC13.1-A1**: The DEC-A sequences with multiple failure events or low frequent fault are identified.*

   - ***Evidence 3.2.3.SC13.1-A1-E1**: DEC-A sequences are identified by PSA analysis and engineering judgment, codes and standards. (See Sub-chapter 13.4.1)*

2) ***Argument 3.2.3.SC13.1-A2**: The DEC-A protection systems are equipped to cope with multiple failure events.*

   - ***Evidence 3.2.3.SC13.1-A2-E2**: DEC-A features are designed to deal with the situations arising from the failure of the safety systems, or initiating events beyond the design basis, and ensure the plant return to safe condition without core damage. (See Sub-chapter 13.4.2)*

3) ***Argument 3.2.3.SC13.1-A3**: In the DEC-A analysis, the key initial parameters, main system parameters and time delay consider the conservative assumptions.*

   - ***Evidence 3.2.3.SC13.1-A3-E1**: The assumptions and input of DEC-A analysis are determined in consideration of conservatism. (See Sub-chapter 13.4.3 and 13.4.4)*

4) ***Argument 3.2.3.SC13.1-A4**: For the DEC-A analysis, the decoupling criteria of DBC-4 mentioned in PCSR Chapter 12 are adopted as strict criteria; therefore, the DEC-A analysis meets the same on and offsite dose targets as the lowest frequency DBC events.*

   - ***Evidence 3.2.3.SC13.1-A4-E1**: The decoupling criteria of DBC-4 mentioned in PCSR Chapter 12 are adopted as strict criteria for the DEC-A analysis. (See Sub-chapter 13.4.3.2)*

   - ***Evidence 3.2.3.SC13.1-A4-E2**: For DEC-A sequences associated with Spent Fuel Pool (SFP), the acceptance criteria are as follows: permanent maintenance of sub-criticality; the fuel assemblies in the SFP remain covered; removal of decay heat from the SFP is ensured. (See*

Sub-chapter 13.4.3.2)

b) ***Sub-Claim 3.4.7.SC13.2: The design and intended operation will return the plant to a safe and stable condition following multiple failure events.***

1) ***Argument 3.4.7.SC13.2-A1****: The DEC-A sequences analysis is performed until the DEC-A final state is reached.*

- ***Evidence 3.4.7.SC13.2-A1-E1****: The final state of DEC-A is proved by sequences analysis. (See Sub-chapter 13.4.5)*

2) ***Argument 3.4.7.SC13.2-A2****: With DEC-A protection systems, the DEC-A sequences are proved to have enough margin.*

- ***Evidence 3.4.7.SC13.2-A2-E1****: The results of DEC-A sequences analysis show margin compared with acceptance criteria. (See Sub-chapter 13.4.5)*

c) ***Sub-Claim 3.2.3.SC13.3: The understanding of severe accident progression and phenomena related to the UK HPR1000 is adequate.***

1) ***Argument 3.2.3.SC13.3-A1****: International research to date on severe accident phenomena is reviewed.*

- ***Evidence 3.2.3.SC13.3-A1-E1****: For UK HPR1000, severe accident sequences are identified and key phenomena related are reviewed. (See Sub-chapter 13.5.2 and 13.5.3)*

2) ***Argument 3.2.3.SC13.3-A2****: Severe Accident Analysis (SAA) modelling and severe accident analysis are performed.*

- ***Evidence 3.2.3.SC13.3-A2-E1****: Unmitigated severe accidents are analysed to reveal potential risks. (See Sub-chapter 13.5.3)*

d) ***Sub-Claim 3.2.3.SC13.4: The analysis codes and models used for SAA are appropriate to simulate severe accident phenomena and progression.***

1) ***Argument 3.2.3.SC13.4-A1****: The analysis codes and models are suitably verified and validated based on the current state of knowledge.*

- ***Evidence 3.2.3.SC13.4-A1-E1****: Codes and models used in SAA are properly validated. (See validation reports of codes used in severe accident analysis)*

- ***Evidence 3.2.3.SC13.4-A1-E2****: The applicability assessment of SAA codes is performed. (See applicability assessment report of codes used in severe accident analysis)*

e) ***Sub-Claim 3.4.7.SC13.5: The severe accident management strategies and engineered measures are proved to be effective and ALARP.***

1) ***Argument 3.4.7.SC13.5-A1****: The Severe Accident Dedicated Valves (SADVs) could effectively avoid high-pressure core melt during a severe accident.*

   - ***Evidence 3.4.7.SC13.5-A1-E1****: Risks related to primary high pressure severe accident are proved to be eliminated by SADVs. (See Sub-chapter 13.5.6.1)*

2) ***Argument 3.4.7.SC13.5-A2****: The Containment Combustible Gas Control System (EUH [CCGCS]) could reduce the hydrogen risk to a safety level that would not challenge the integrity of containment.*

- ***Evidence 3.4.7.SC13.5-A2-E1****: The effectiveness of EUH [CCGCS] is proved by analysis with lumped parameter method and Computational Fluid Dynamics (CFD) method. (See Sub-chapter 13.5.6.2)*

3) ***Argument 3.4.7.SC13.5-A3****: The In-Vessel Retention (IVR) strategy could maintain the integrity of reactor vessel after core melt.*

   - ***Evidence 3.4.7.SC13.5-A3-E1****: Comprehensive analysis about IVR is performed to show that reactor vessel can maintain its integrity. (See Sub-chapter 13.5.6.3)*

4) ***Argument 3.4.7.SC13.5-A4****: The Containment Heat Removal System (EHR [CHRS]) system could maintain the temperature and pressure of containment below design basis.*

   - ***Evidence 3.4.7.SC13.5-A4-E1****: The containment pressure and temperature are proved to be low enough than design basis when EHR [CHRS] is effective. (See Sub-chapter 13.5.6.4)*

5) ***Argument 3.4.7.SC13.5-A5****: The Containment Filtration and Exhaust System (EUF [CFES]) system could maintain the confinement function of containment and avoid the overpressure failure risk.*

   - ***Evidence 3.4.7.SC13.5-A5-E1****: The containment pressure can be controlled lower than design pressure when EUF [CFES] is effective. (See Sub-chapter 13.5.6.5)*

6) ***Argument 3.4.7.SC13.5-A6****: The other mitigation measures excluding dedicated severe accident mitigation systems are effective.*

   - ***Evidence 3.4.7.SC13.5-A6-E1****: Potential risks that may lead to large or early radioactive release are practically eliminated. (See Sub-chapter 13.5.8)*

f) *Sub-Claim 3.4.7.SC13.6: UK HPR1000 is capable to deal with extreme events like Fukushima accident.*

1) ***Argument 3.4.7.SC13.6-A1****: System design in UK HPR1000 takes account of*

the lessons learnt from the Fukushima accident.

- ***Evidence 3.4.7.SC13.6-A1-E1**: Lessons from Fukushima accident are also addressed in the design of UK HPR1000. (See Sub-chapter 13.5.11)*

g) ***Sub-Claim 3.4.7.SC13.7: The behaviour of fission products during a severe accident is properly considered.***

1) ***Argument 3.4.7.SC13.7-A1**: The source term analysis codes and models are suitable.*

- ***Evidence 3.4.7.SC13.7-A1-E1**: Codes and models used in severe accident source term analysis are properly validated. (See validation reports of codes used in severe accident analysis)*

2) ***Argument 3.4.7.SC13.7-A2**: The chemical form, possible release categories, magnitude and timing are identified.*

- ***Evidence 3.4.7.SC13.7-A2-E1**: Fission products behaviours and release categories are properly considered in severe accident source term analysis. (See Sub-chapter 13.5.7)*

3) ***Argument 3.4.7.SC13.7-A3**: The design features of the UK HPR1000 and their functions for radionuclides retention and transport are analysed.*

- ***Evidence 3.4.7.SC13.7-A3-E1**: The effects of UK HPR1000 on source term analysis are modelled to get reasonable source term results. (See Sub-chapter 13.5.7)*

The structure and contents of Claims - Arguments - Evidence (CAE) for this chapter will be improved all through the GDA steps.

13.2.2 Chapter Structure

The general structure of this chapter is presented below:

a) Sub-chapter 13.1 - lists all the Abbreviations and Acronyms which are presented in this chapter.

b) Sub-chapter 13.2 - introduces the route map, structure, interfaces with other chapters, and the strategy of this chapter.

c) Sub-chapter 13.3 - presents the relevant codes and standards of DEC-A and severe accident analysis.

d) Sub-chapter 13.4 - presents the methodology and results of DEC-A sequence identification and analysis.

e) Sub-chapter 13.5- presents the severe accident mitigation measures coping with DEC-B events and methodology and the results of DEC-B analysis.

f) Sub-chapter 13.6 - presents the ALARP evaluation.

g) Sub-chapter 13.7 - presents concluding remarks.

h) Sub-chapter 13.8 –lists the references.

i) Appendix 13A – provides the introduction to computer codes used in DEC-A and DEC-B analysis.

13.2.3 Interfaces with Other Chapters

The interfaces with other Chapters are listed in the following table.

T-13.2-1 Interfaces between Chapter 13 and Other Chapters

PCSR Chapter	Interface
Chapter 1	Chapter 1 provides the Fundamental Objective, Level 1 Claims and Level 2 Claims. Chapter 13 provides chapter claims and arguments to support relevant claims that are addressed in Chapter 1.
Chapter 3	PCSR Chapter 3 provides inputs to the safety evaluation reference for Design Extension Conditions and Severe Accident Analysis presented in Chapter 13.
Chapter 4	Chapter 4 provides the general principles for safety analysis.
Chapters 6~11	Provide the substantiation of the Reactor Coolant System, Safety Systems, Instrumentation & Controls, Electric Power, Auxiliary Systems and Steam & Power Conversion System, which are taken into consideration for the Design Extension Condition analysis.
Chapter 12	Chapter 12 provides initiating events for DEC-A sequences identification and acceptance criteria of DBC-4 for DEC-A analysis.
Chapter 14	Chapter 14 provides PSA results to support the identification of DEC-A and DEC-B events and shows that the total risks and exposure of public and workers from DEC-A and DEC-B events can meet specified Radiation Protection Targets (RPTs). Chapter 13 provides the thermal-hydraulic analysis results and source term input to PSA.

PCSR Chapter	Interface
Chapter 15	Chapter 15 substantiates the claims on operator actions under DEC-A and severe accident conditions. Chapter 13 provides human-related claims (implied and explicit) in the SAA, which need Suitably Qualified and Experienced Person (SQEP) Human Factors (HF) analysis and/or review.
Chapter 16	Chapter 16 presents the design substantiation of civil structures. PCSR Chapter 13 provides thermo-hydraulic condition in internal containment under severe accident for design of civil structures.
Chapter 18	Chapter 18 provides external hazards as an input to identify parts of DEC events considered in Chapter 13.
Chapter 21	Chapter 13 provides accident process for DEC-A and DEC-B events, and source term of fission product and combustible gases to support the understanding of accident chemistry.
Chapter 22	Chapter 13 provides DEC-A and severe accident source terms.
Chapter 28	Chapter 13 provides analysis results of fuel route and storage to support the ALARP evaluation.
Chapter 31	Chapter 13 provides the framework and information of severe accident management guidelines described in chapter 31.
Chapter 32	Chapter 13 provides the basic strategy of Severe Accident Management Guidelines (SAMGs) for Emergency Arrangements.
Chapter 33	The ALARP assessment approach presented in Chapter 33 is applied in Chapter 13, which will support the overall ALARP evaluation.

13.3 Applicable Codes and Standards

For the UK HPR1000, the codes and standards applied are selected and reviewed

according to the principles described in PCSR Chapter 4 and the *General Principles for Application of Laws, Regulations, Codes and Standards* [2]. For DEC analysis, the following related codes and standards are identified, which are mainly guidance documents. The suitability and compliance of these guidance documents are assessed [3].

T-13.3-1 Applicable Codes and Standards

1.	Design Extension of Existing Reactors, WENRA GUIDANCE DOCUMENT ISSUE F, 2014.
2.	Considerations on Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA TECDOC-1791, 2016.
3.	Safety Assessment for Facilities and Activities, IAEA GSR Part 4, 2016.
4.	Safety of Nuclear Power Plants: Design, IAEA SSR-2/1 (Rev.1), 2016.
5.	Design of Reactor Containment Systems for Nuclear Power Plants, IAEA NS-G-1.10, 2004.
6.	Deterministic Safety Analysis for Nuclear Power Plants, IAEA SSG-2, 2009.
7.	Standard Review Plan, NRC NUREG-0800, 2007.
8.	Approaches and Tools for Severe Accident Analysis for Nuclear Power Plants, IAEA Safety Reports Series NO.56, 2008.
9.	Severe Accident Management Programmes for Nuclear Power Plants, IAEA NS-G-2.15, 2009.

13.4 DEC-A Analysis

13.4.1 DEC-A Sequences Identification

The requirement and methodology for DEC-A sequences identification is described in Sub-chapter 13.4.1.1. The list of identified DEC-A sequences of the UK HPR1000 is shown in Sub-chapter 13.4.1.2.

13.4.1.1 Requirement and Methodology of DEC-A Sequences Identification

A set of DECs are derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These DECs are used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their

consequences.

The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant could prevent accident conditions that are beyond design basis accident conditions, or to mitigate their consequences, so far as is reasonably practicable.

The process of DEC-A sequences identification considers the following methods [4]:

a) Referring to the sequences suggested or required in the codes and standards.

b) Referring to the results from the PSA analysis.

c) Referring to engineering judgment and operating experience.

13.4.1.2 DEC-A Sequences List

Based on the identification process which is addressed in Reference [5] the DEC-A list is identified by PSA analysis and engineering judgment, codes and standards. The DEC-A list for UK HPR1000 is provided in T-13.4-1 below.

T-13.4-1 DEC-A Sequences Considered in the UK HPR1000 [6]

No.	Event Description	Safety Analysis States
1	Total Loss of Feedwater (TLOFW)	A
2	Small Break - Loss of Coolant Accident (SB-LOCA) with Failure of Medium Pressure Rapid Cooldown (MCD)	A
3	SB-LOCA with Total Loss of Low Head Safety Injection (LHSI)	A
4	SB-LOCA with Total Loss of LHSI (Shutdown Condition)	C/D
5	Loss of Residual Heat Removal (RHR) or Failure of Recovery of RHR after Loss of Offsite Power (LOOP)	C/D
6	Station Black Out (SBO)	A\B\C\D\E\F
7	Anticipated Transient Without Scram (ATWS) Due to Protection System (RPS [PS]) Failure	A
8	ATWS Due to Failure of Rod Cluster Control Assembly (RCCA) to Insert, including：	A

No.	Event Description	Safety Analysis States
	a) ATWS by Rods Failure-LOOP. b) ATWS by Rods Failure- SB-LOCA. c) ATWS by Rods Failure-Loss of Main Feedwater. d) ATWS by Rods Failure-Excessive Increase in Secondary Steam Flow. e) ATWS by Rods Failure-Spurious Pressuriser Spraying. f) ATWS by Rods Failure-Steam Line Break in Downstream of Main Steam Isolation Valve (MSIV).	
9	SB-LOCA with Total Loss of Medium Head Safety Injection (MHSI)	A
10	Total Loss of Cooling Chain (TLOCC) with Reactor Coolant Pump Sealing Leakage	A
11	TLOCC (Shutdown Condition)	C/D
12	Loss of Three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) Trains	A\B\C\D\E\F
13	Loss of Ultimate Heat Sink (LUHS) for 100 Hours	A/B
14	Uncontrolled Primary Water Level Drop without Safety Injection Signal from RPS [PS]	C/D
15	Multiple Steam Generator Tubes Rupture (SGTR) (10 tubes)	A
16	Main Steam Line Break (MSLB) with SGTR (1 tube) in the Affected Steam Generator (SG)	A
17	SGTR (1 tube) with Atmospheric Steam Dump System (VDA [ASDS]) Stuck Open in the Affected SG	A
18	TLOCC with Loss of Secondary Cooldown (failure of Emergency Feedwater System (ASG [EFWS]) or VDA [ASDS])	A

Notes:

Events postulated in safety analysis are supposed to occur during normal plant operation. The initiating conditions assumed in safety analysis cover all the possible standard conditions from full power operation to cold shutdown. The definitions of the Safety Analysis States for UK HPR1000 are described in PCSR Chapter 12.

13.4.2 DEC-A Features

DEC-A features are designed to deal with the situations arising from the failure of the safety systems, or initiating events beyond the design basis, and ensure the plant return to safe condition without core damage. These features aim to prevent a core damage situation that would have otherwise occurred.

The identified DEC-A sequences with similar functional characteristics can be protected by the same DEC-A features. The features are introduced as follows.

a) Extra Cooling System (ECS [ECS]):

The ECS [ECS] is designed to provide extra cooling source for EHR [CHRS] and PTR [FPTCS] if they are operating or required to be actuated in the case of loss of Component Cooling Water System (RRI [CCWS]) and/or the Essential Service Water System (SEC [ESWS]).

During TLOCC in state A with Reactor Coolant System (RCP [RCS]) pump sealing break and TLOCC/SBO in state D, the operator opens the EHR [CHRS] and ECS [ECS] to limit pressure increase in the containment and ensure the In-containment Refuelling Water Storage Tank (IRWST) cooling. The ECS [ECS] is used to cool the EHR [CHRS], which is regarded as the final heat sink for the containment. In the case of SBO in SFP, the ECS [ECS] is actuated to cool PTR [FPTCS] and remove the decay heat in spent fuel.

The cooling function of ECS [ECS] is guaranteed for 3 hours after the accident.

b) EHR [CHRS]:

The DEC-A function of EHR [CHRS] is considered to limit the pressure increase of containment and ensure IRWST cooling when RHR fails.

During TLOCC in state A or state D, SBO in state D, SB-LOCA with total loss of Low Head Safety Injections (LHSIs) in state A and state D, and Loss of RHR or failure of recovery of RHR after LOOP in state D, EHR [CHRS] is actuated to reduce the containment pressure and to limit the IRWST water temperature to avoid the cavitation of LHSI pumps.

c) SBO Diesel Generators (DGs):

In the case of SBO during all operation modes, the two SBO DGs are assumed to be actuated manually by the operator 30 minutes after the first significant signal (e.g. Reactor Trip (RT) signal) to supply electricity to the necessary safety systems and

relevant auxiliary systems. During SBO accidents in state A, the 2 trains of ASG [EFWS] and VDA [ASDS] are powered by SBO DGs to ensure the heat removal from the primary system. For SBO accidents in state D, the LHSI and Safety Chilled Water System (DEL [SCWS]) are powered by SBO DGs to ensure the inventory of primary system, the EHR [CHRS] and ECS [ECS] are supplied by SBO DGs to ensure the heat removal in the long time. For SBO accidents in SFP, the PTR [FPTCS] and ECS [ECS] need a power supply to ensure the SFP cooling.

d) Diverse Actuation System (KDS [DAS]):

The KDS [DAS] is designed to deal with DEC-A sequences which result from failure of the RPS [PS]. During ATWS accidents due to signal failure, the diverse RT signals are designed for the reactor trip. For the uncontrolled primary water level drop without Safety Injection (SI) signal from RPS [PS], the “RCP [RCS] loop level low 1” signal is designed to actuate Safety Injection System (RIS [SIS]).

e) Emergency Boration System (RBS [EBS]):

RBS [EBS] is designed to provide sufficient boration and to ensure subcritical conditions in accidents. The RBS [EBS] system is designed to actuate automatically by the ATWS signal. In addition, the RBS [EBS] is used to ensure core subcritical conditions during the cooling process of primary system.

f) Safety Chilled Water System (DEL [SCWS]):

In the case of RRI [CCWS] and/or SEC [ESWS] failure, the DEL [SCWS] can offer a diverse cooling chain to cool the LHSI pump motors so as to ensure the normal operation of LHSI pumps. During TLOCC accidents in state A or state D, the diverse cooling chain can be connected to LHSI pumps automatically by the high temperature or low flowrate signal of RRI [CCES]. During SBO in state D, the diverse cooling chain can be connected to LHSI pumps 30 minutes after the first significant signal to ensure the cooling of LHSI pump motors.

g) Manual feed and bleed operation:

In the case of SB-LOCA accidents with failure of MCD in state A, the core melt can be prevented by removing the decay heat via the manual feed and bleed operation, which consists of RIS [SIS] actuation and opening of three trains of Pressuriser (PZR) safety valves. For total loss of RHR accidents in shutdown states with failure of secondary side heat removal, core residual heat can be removed effectively through manual feed and bleed operation. In addition, during TLOFW accidents in state A, manual feed and bleed operation is regarded as a main and effective measure to deal with the accident.

Manual feed and bleed operation can be carried out by the operator under the following conditions: very low SG level in three Steam Generators (SGs), core outlet temperature higher than 330°C, loss of Turbine Bypass System (GCT [TBS]) and

VDA [ASDS], total loss of RHR and secondary side heat removal in shutdown states, etc.

h) Low Pressure Full Cooldown (LCD):

LCD is designed to depressurise the primary pressure rapidly for the efficient injection of LHSI during DEC-A conditions.

In the case of SB-LOCA with total loss of MHSI, LCD is performed to ensure the primary side is depressurised down to the LHSI injection pressure. This function is realised by operators via the stepwise pressure setpoint reduction leading to full opening of all VDA [ASDS].

i) Secondary Passive Heat Removal System (ASP [SPHRS]):

The ASP [SPHRS] is designed as the secondary passive system to remove the core decay heat when the secondary active heat removal system fails.

In the case of TLOFW, the ASP [SPHRS] can be used to remove the core residual heat effectively and continually in the long term to avoid core melt. It will be actuated automatically 60s after the “SG level (wide range) low 3” signal and all the feedwater flow rates of ASG [EFWS] are low. However, as the function classification of this function is FC3, it is not claimed to be used during the TLOFW accident analysis.

In addition, the ASP [SPHRS] tank water is used as the water source to feed the ASG [EFWS] tank in the long term of the SBO or LUHS accident. It is also used as the water source to feed the SFP during the Loss of Three PTR [FPCTS] Trains accident.

To demonstrate the effectiveness of DEC-A features, DEC-A analysis will be performed in Sub-chapter 13.4.5. The aims for DEC-A features are as follows:

a) Prevent core damage.

b) Return the plant to a safe or controllable state.

c) Ensure that the DBC-4 success criteria (see Chapter 12) are met and thereby ensure that there is no cliff-edge just beyond the design basis.

13.4.3 DEC-A Analysis Methodology

13.4.3.1 Main Assumptions for DEC-A Analysis

In the DEC-A analysis, the key initial parameters, main system parameters and time delay consider the conservative assumptions. However, LOOP and single failure are not considered during DEC-A analysis. Preventive maintenance for safety systems is not taken into consideration during the DEC-A accident analysis [7].

a) Input Parameters

The key initial parameters of steady-state conditions are penalised by considering

their uncertainties for DEC-A analysis.

b) System Availability and Assumptions

Equipment that is not qualified for specific accident conditions is assumed to fail unless its continued operation results in more unfavourable conditions. The DBC safety functions are considered to be available during the DEC-A analysis unless they are assumed to fail as an assumption of the DEC-A sequences. During the DEC-A analysis, specific DEC-A functions are also considered. For these DBC or DEC-A protection systems, conservative assumptions are applied to their operation parameters.

The normal operation systems including control systems are not credited in the analysis of DEC-A, unless they are qualified to be available. However, if normal operation systems have a negative impact during the course of the DEC-A accident, they are considered as part of the analysis.

Non-permanent equipment, such as mobile power and mobile pumps, is not considered for demonstration of the adequacy of DEC-A measures. Such equipment is considered for the operator to operate as part of a long-term sequence and the time claimed for availability of non-permanent equipment is justified.

c) Operator Actions

In the DEC-A analysis, manual actions initiated from the Main Control Room (MCR) are assumed to be performed 30 minutes after the first significant signal (such as a RT signal). Local manual actions are assumed to be performed 60 minutes after the first significant signal.

13.4.3.2 Acceptance Criteria for DEC-A Analysis

The decoupling criteria of DBC-4 mentioned in PCSR Chapter 12 are adopted as strict criteria for the DEC-A analysis [7].

In addition, the acceptance criteria for DEC-A sequences associated with SFP are as follows:

a) Permanent maintenance of sub-criticality.

b) The fuel assemblies in the SFP remain covered.

c) Removal of decay heat from the SFP is ensured.

13.4.3.3 DEC-A Final State

DEC-A analysis is performed until the safe state called “DEC-A final state” is reached. The DEC-A final state is defined as follows [7]:

a) The core and SFP fuel assemblies remain sub-critical.

b) Continuous removal of heat from the reactor core and from the SFP is ensured.

c) Confinement of radioactive material is ensured.

In addition, as described in PCSR Sub-chapter 12.10, analyses of some DEC-A sequences can support demonstration of diverse protection lines. For these sequences, analyses are performed until the safe state is reached. The definition of safe state is shown in PCSR Chapter 12.5.2.

13.4.4 DEC-A Key Inputs

The input parameters and uncertainties for the DEC-A analysis are provided in the report *NSSS Operating Parameters*, Reference [8].

13.4.5 DEC-A Sequences Analysis

In this Sub-chapter, the DEC-A sequences listed in 13.4.1.2 are analysed to demonstrate that the DEC-A provisions are effective.

13.4.5.1 TLOFW (State A)

13.4.5.1.1 Description

TLOFW accident refers to the loss of the Main Feedwater Flow Control System (ARE [MFFCS]), Startup and Shutdown Feedwater System (AAD [SSFS]) and ASG [EFWS] simultaneously. TLOFW is classified as a DEC-A accident.

When a TLOFW accident occurs, the feedwater supply of the SG will be completely interrupted. The primary pressure will increase due to the insufficient secondary heat removal. When the primary pressure rises to the set-point of Pressuriser Safety Valve (PSV), the PSV is automatically actuated to prevent the RCP [RCS] overpressure. Because of the discharged coolant through PSV, the core exposure and heat-up may occur.

In order to mitigate the accident, the DEC-A feature feed and bleed operation should be performed by the operator as a key measure. Three trains of Pressuriser Safety Valves (PSVs) are manually opened to depressurise the primary system. The loss of coolant inventory is compensated by the RIS [SIS]. In the long term, the decay heat is removed through the RHR.

13.4.5.1.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as a target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.1.3 Main Safety Functions

The following safety functions and operator actions are claimed in the analysis of TLOFW:

a) Automatic functions

1) RT

The RT is triggered by the “SG Level (Narrow Range (NR)) Low 1” signal (FC1).

2) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

3) VDA [ASDS]

Three trains of VDA [ASDS] automatically open when the SG pressure reaches “SG pressure high 1” (FC1).

4) PSV

The PSVs automatically open when the opening set-point is reached (FC1).

5) SI signal

The SI signal is triggered by the “Pressuriser pressure low 3” signal (FC1).

6) Shutdown of RCP [RCS] pumps

The RCP [RCS] pumps stop due to the “SG level (Wide Range (WR)) low 4” signal (FC1).

b) Operator actions

1) Shutdown of PZR heaters

The PZR heaters are manually cut off (FC2).

2) Feed and bleed

This safety function is a DEC-A feature. The operator opens 3 trains of PSVs to

initiate feed and bleed when the core outlet temperature exceeds 330°C (FC2).

In this accident, the DEC-A feature feed and bleed operation is a key mitigation measure, which depressurises the primary system and removes the decay heat.

3) Accumulators isolation

During the RCP [RCS] depressurisation, the accumulators are isolated when the reactor coolant system pressure falls below 2.0 MPa abs (FC2).

4) RIS [SIS] in RHR mode

The RHR is connected to the RCP [RCS] to ensure continuous heat removal and long-term core cooling (FC2).

13.4.5.1.4 Typical Events Sequences

The TLOFW event occurs with the interruption of feedwater supply of SGs, which is led by the loss of ARE [MFFCS], AAD [SSFS] and ASG [EFWS].

The water inventory of SGs rapidly decreases after the accident occurs. When the SG level decreases to “SG level (NR) low 1”, the RT is triggered. The turbine trip is actuated concurrently with RT. After the turbine trip, the SG pressure increases and the opening set-point of VDA [ASDS] is reached. The VDA [ASDS] automatically opens to prevent secondary overpressure.

Due to the discharged water inventory through VDA [ASDS], the SG water level decreases continuously. When “SG level (WR) low 2” signal is triggered, the blowdown pipeline of Steam Generator Blowdown System (APG [SGBS]) is isolated. When “SG level (WR) low 4” is reached, the RCP [RCS] pumps stop to reduce heat generation in primary system.

Along with the reducing water level of SGs, the primary pressure and coolant temperature gradually rise due to the insufficient heat removal through the secondary side. PSVs automatically open when the primary pressure reaches the opening set-point, thus primary overpressure is avoided. However, the coolant is discharged through PSVs and so core exposure and heat-up may occur.

Manual actions are performed by the operator to mitigate the accident. 30 minutes after the RT signal, the operator manually cuts off the PZR heaters. When the core outlet temperature exceeds 330°C, at the earliest 30 minutes after the RT signal, the operator opens 3 trains of PSVs to initiate feed and bleed operation.

The opening of PSVs results in the fast depressurisation of primary system and the discharge of coolant. The primary pressure rapidly decreases to the “Pressuriser pressure low 3” threshold, where the SI signal is triggered. The MHSI or LHSI starts to inject borated water into the RCP [RCS] as soon as the injection pressure is reached. The core level begins to recover with the water compensation and the core heat-up is

prevented. The decay heat is removed through the feed and bleed operation, which causes the primary pressure and coolant temperature to decrease. When the RIS [SIS] connection condition in RHR mode is met, the final state of DEC-A is reached.

13.4.5.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [9]. The main assumptions are as follows:

a) The TLOFW accident is assumed to occur at full power state.

b) Initial reactor power is 102% Full Power (FP), which is considered to maximise primary heat.

c) The reactor loop flowrate is the thermal design flowrate, which is considered to penalise heat removal.

d) The Reactor Pressure Vessel (RPV) coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial Pressuriser pressure is the nominal value minus the maximum uncertainty, which is considered to penalise heat removal through the automatic opening of the PSVs.

f) The initial Pressuriser level is the nominal level at power minus 7% based on uncertainties, which is considered to penalise water inventory.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise water inventory of secondary system.

h) The core bypass flowrate is maximum, which is considered to penalise heat removal.

i) After the RT, a conservative heat curve (1.645σ uncertainties on the “B+C term”) is used for the core decay heat.

13.4.5.1.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [9]. In the transient of TLOFW, the analysis indicates that the peak cladding temperature is 355 °C, which is much lower than the requirements (1204 °C) in acceptance criteria. The maximum cladding oxidation is 0.006% of the cladding thickness, which is much lower than the requirements (17%) in acceptance criteria. The hydrogen generation is 0.004% of the amount that would have been generated if the whole active part of the cladding had reacted, which is far less than the requirements (1%) in acceptance criteria. The acceptance criteria are met. When the RIS [SIS] connection condition in RHR mode is met, the decay heat removal is ensured by the RHR in the long term.

The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.2 SB-LOCA with Failure of MCD (State A)

13.4.5.2.1 Description

SB-LOCA with Failure of MCD is classified as a DEC-A accident, which is initiated by a small break located at the cold leg. The break size is considered as equivalent diameters of 2.5 cm and 5.0 cm. The MCD is assumed to fail because of the failure of GCT [TBS] and VDA [ASDS].

When SB-LOCA occurs, the break leads to the decrease of coolant inventory which cannot be compensated by the Chemical and Volume Control System (RCV [CVCS]). The primary pressure reduces and the RT signal and SI signal are triggered in sequence. The SI signal also triggers the MCD, however it fails to be actuated due to the loss of GCT [TBS] and VDA [ASDS]. The SG pressure is limited by the Main Steam Safety Valve (MSSV).

Because of the failure of MCD, the primary pressure remains high and the RIS [SIS] cannot perform injection. The DEC-A feature feed and bleed operation is performed by the operator as a key mitigation measure. Three trains of PSVs are manually opened to depressurise the primary system. The primary pressure decreases rapidly. The RIS [SIS] starts to inject water into the RCP [RCS] to compensate the coolant inventory. In the long term, the decay heat is removed through the RHR.

13.4.5.2.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as a target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and

Sub-chapter 13.4.7.

13.4.5.2.3 Main Safety Functions

The following safety functions and operator actions are claimed in the analysis of SB-LOCA with failure of MCD.

a) Automatic protections

1) RT

The RT is triggered by the “Pressuriser pressure low 2” signal (FC1).

2) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

3) Isolation of ARE [MFFCS] full load line

After RT, the full load isolation valves of the ARE [MFFCS] are closed (FC1).

4) SI signal

The SI signal is triggered by the “Pressuriser pressure low 3” signal (FC1).

5) Shutdown of RCP [RCS] pumps

The RCP [RCS] pump trip is triggered by co-existence of “RCP [RCS] Pumps ΔP low 1” signal and SI signal in two loops (FC1).

6) MSSV

The Main Steam Safety Valves (MSSVs) automatically open when the opening set-point is reached (FC1).

7) ASG [EFWS]

The ASG [EFWS] are actuated on “SG level (WR) low 2” signal (FC1).

b) Operator actions

1) Feed and bleed

The operator opens 3 trains of PSVs to actuate feed and bleed. This safety function is a DEC-A feature (FC2).

In this accident, the DEC-A feature feed and bleed operation is a key mitigation measure, which depressurises the primary system and ensures the effective injection of the RIS [SIS].

2) Accumulators isolation

During the RCP [RCS] depressurisation, the accumulators are isolated when the reactor coolant system pressure decreases below 2.0 MPa abs (FC2).

3) RIS [SIS] in RHR mode

The RHR is connected to the RCP [RCS] to ensure continuous heat removal and core long-term cooling (FC2).

13.4.5.2.4 Typical Events Sequences

The accident is initiated by a small break located at the cold leg. The break size is considered with equivalent diameters of 2.5 cm and 5.0 cm. The loss of coolant inventory cannot be compensated by RCV [CVCS].

The discharged coolant through the break leads to a decrease of primary pressure. The RT is triggered by “Pressuriser pressure low 2” signal. Then the turbine trip occurs and the ARE [MFFCS] full load isolation valves are closed concurrently with RT. In the analysis of this accident, it is conservatively assumed that the low load pipelines of the ARE [MFFCS] are unavailable, and the ASG [EFWS] is used to control the SG level. Because of the loss of GCT [TBS] and VDA [ASDS], the MSSVs automatically open to prevent overpressure of secondary system. The PZR heaters are automatically switched off by “Pressuriser level low 3” signal.

When the primary pressure decreases to “Pressuriser pressure low 3” threshold, the SI signal is triggered. The RCP [RCS] pumps shutdown is triggered by coincident signals: RCP [RCS] Pumps ΔP low 1 signal and SI signal in two loops.

The SI signal also triggers the MCD. However, the MCD fails to be actuated and the primary system still remains high. In order to depressurise the RCP [RCS] and ensure the effective injection of the RIS [SIS], manual actions are performed by the operator. 30 minutes after the RT signal, the operator manually opens three trains of PSVs to initiate the feed and bleed operation.

The opening of the PSVs results in the fast depressurisation of primary system and the discharge of coolant. The MHSI or LHSI starts to inject borated water into the RCP [RCS] as soon as the injection pressure is reached. The core level begins to recover with the water compensation and the core heat-up is prevented. The decay heat is removed through the feed and bleed operation and the primary pressure and coolant temperature decrease. When the RIS [SIS] connection condition in RHR mode is met, the final state of DEC-A is reached.

13.4.5.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [10]. The main assumptions are as follows:

a) The accident is assumed to occur at full power state.

b) Initial reactor power is 102% FP, which is considered to maximise primary heat.

c) The reactor loop flowrate is the thermal design flowrate, which is considered to

penalise heat removal.

d) The RPV coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial pressuriser pressure is the nominal value plus the maximum uncertainty, which is considered to delay RT and SI signal.

f) The initial pressuriser level is the nominal level at power minus 7% based on uncertainties, which is considered to penalise water inventory.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise water inventory of secondary system.

h) The core bypass flowrate is maximum, which is considered to penalise heat removal.

i) After the RT, a conservative curve (2σ uncertainties on the "B+C term") is used for the core decay heat.

13.4.5.2.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [10]. In the case of 2.5 cm equivalent diameter break, the peak cladding temperature is 357 °C, which is much lower than the requirements (1204 °C) in the acceptance criteria. The maximum cladding oxidation is 0.004% of the cladding thickness, which is much lower than the requirements (17%) in the acceptance criteria. The hydrogen generation is 0.003% of the amount that would have been generated if the whole active part of the cladding had reacted, which is far less than the requirements (1%) in the acceptance criteria. The acceptance criteria are met.

In the case of 5.0 cm equivalent diameter break, the peak cladding temperature is 368 °C, which is much lower than the requirements (1204 °C) in the acceptance criteria. The maximum cladding oxidation is 0.006% of the cladding thickness, which is much lower than the requirements (17%) in the acceptance criteria. The hydrogen generation is 0.003% of the amount that would have been generated if the whole active part of the cladding had reacted, which is far less than the requirements (1%) in the acceptance criteria. The acceptance criteria are met.

When the RIS [SIS] connection condition in RHR mode is met, the decay heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.3 SB-LOCA with Total Loss of LHSI (State A)

13.4.5.3.1 Description

SB-LOCA with total loss of LHSI is classified as a DEC-A accident, which is initiated

by a small break located at the cold leg. The break size is considered with equivalent diameters of 2.5 cm and 5.0 cm. The LHSI is assumed to be unavailable.

When SB-LOCA occurs, the break leads to the decrease of coolant inventory which cannot be compensated by RCV [CVCS]. The primary pressure reduces, the RT signal and SI signal are triggered in sequence. The SI signal also triggers MCD, which depressurises the RCP [RCS] to allow the injection of MHSI. The MHSI compensates the loss of coolant inventory.

Until this state, the decay heat is largely transferred into the IRWST through the break flow, which could lead to the increase of IRWST water temperature and the loss of MHSI. Three trains of VDA [ASDS] are manually opened by the operator to perform the manual cooldown. The primary system is depressurised and the decay heat is partly removed via the secondary side. Due to the loss of LHSI, the RHR is unavailable. The EHR [CHRS] is used to ensure the cooling of the IRWST and control the containment pressure. The cavitation of the MHSI pumps is prevented. In the long term, the coolant inventory is maintained by the MHSI. The decay heat is removed through the EHR [CHRS] and the secondary side.

For SB-LOCA, the core exposure and heat-up led by the loss of coolant inventory is the main potential consequence. Compared with the case of 2.5 cm break, the break mass flow is larger in the case of 5.0 cm break. With the same mitigation strategy, the case of 5.0 cm break is considered as the bounding one since it leads to a greater loss of the coolant and is more challenging to the acceptance criteria. Therefore, the case of 5.0 cm break is analysed as the bounding case.

13.4.5.3.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.3.3 Main Safety Functions

The following safety functions are claimed in the analysis of SB-LOCA with total loss of LHSI.

a) Automatic protections

1) RT

The RT is triggered by the “Pressuriser pressure low 2” signal (FC1).

2) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

3) Isolation of ARE [MFFCS] full load line

After RT, the full load lines of the ARE [MFFCS] are isolated (FC1).

4) SI signal

The SI signal is triggered by the “Pressuriser pressure low 3” signal (FC1).

5) MCD

The MCD is initiated by SI signal to cool down the primary system with a cooling rate of 250 °C/h (FC1).

6) Shutdown of RCP [RCS] pumps

The RCP [RCS] pump trip is triggered by co-existence of RCP [RCS] Pumps ΔP low 1 signal and SI signal in two loops (FC1).

7) VDA [ASDS]

Three trains of VDA [ASDS] automatically open when the SG pressure reaches “SG pressure high 1” (FC1).

8) ASG [EFWS]

The ASG [EFWS] are actuated on “SG level (WR) low 2” signal. The isolation of ASG [EFWS] is actuated by “SG level (WR) high 1”signal (FC1).

b) Operator actions

1) RCP [RCS] boration

Two trains of RBS [EBS] are actuated by the operator to borate the RCP [RCS] (FC2).

2) Manual cooldown of the primary system.

Three trains of VDA [ASDS] are manually opened to perform the cooldown of primary system { } (FC2).

3) Accumulators isolation

During the RCP [RCS] depressurisation, the accumulators are isolated when the primary pressure decreases below 2.0 MPa abs (FC2).

4) Manual EHR [CHRS] actuation

The EHR [CHRS] in spraying mode is manually actuated on the signal of high containment pressure or high water temperature of IRWST. This safety function is a DEC-A feature (FC3).

13.4.5.3.4 Typical Events Sequences

The accident is initiated by a small break located at the cold leg. The break size is considered as equivalent diameters of 2.5 cm and 5.0 cm. The bounding case of 5.0 cm break is analysed. The loss of coolant inventory cannot be compensated by RCV [CVCS].

The discharged coolant through the break leads to a decrease of primary pressure. The RT is triggered by “Pressuriser pressure low 2” signal. Then the turbine trip occurs and the ARE [MFFCS] full load isolation valves are closed coincident with RT. In the analysis of this accident, it is conservatively assumed that the low load pipelines of the ARE [MFFCS] are unavailable, and the ASG [EFWS] is used to control the SG level. The SG pressure rapidly increases to the “SG pressure high 1” threshold after the turbine trip, at which point the VDA [ASDS] automatically opens to prevent overpressure of the secondary side. The PZR heaters are automatically switched off by “Pressuriser level low 3” signal.

When the primary pressure decreases to the “Pressuriser pressure low 3” threshold, the SI signal is triggered. The RCP [RCS] pumps shutdown is triggered by co-existence of RCP [RCS] Pumps ΔP low 1 signal and SI signal in two loops. The SI signal activates MHSI and LHSI. However, the LHSI fails to actuate. The SI signal also triggers the MCD. The MCD cools down and depressurises the primary system with a cooling rate of 250 °C/h. During the MCD, the MHSI injection pressure is reached and the coolant inventory is compensated by the MHSI. The RPV water level starts to recover.

Manual actions are performed by the operator to mitigate the accident. Two RBS [EBS] pumps are manually actuated to inject borated water into the RCP [RCS]. Three trains of VDA [ASDS] are manually opened to depressurise the primary system. The accumulators start to inject water into the RCP [RCS] as soon as the injection pressure is reached. The decay heat is continuously removed through the secondary side. The pressure and temperature of the primary system decrease during the RCP [RCS] depressurisation.

The decay heat is largely transferred into the IRWST through the break flow. The pressure and temperature of the containment gradually increase. After the containment pressure increases to 0.1464 MPa, the EHR [CHRS] is manually actuated to maintain the IRWST water temperature and the integrity of containment. In the long term, the decay heat is removed via the EHR [CHRS] and secondary side. The final state is reached.

13.4.5.3.5 Analysis Assumptions

The detailed assumptions are presented in Reference [11]. The main assumptions are as follows:

a) The accident is assumed to occur at full power state.

b) Initial reactor power is 102% FP, which is considered to maximise primary heat.

c) The reactor loop flowrate is the thermal design flowrate, which is considered to penalise heat removal.

d) The RPV coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial pressuriser pressure is the nominal value plus the maximum uncertainty, which is considered to delay RT and SI signal.

f) The initial pressuriser level is the nominal level at power minus 7% based on uncertainties, which is considered to penalise water inventory.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise water inventory of secondary system.

h) The core bypass flowrate is maximum, which is considered to penalise heat removal.

i) After the RT, a conservative curve (2σ uncertainties on the “B+C term”) is used for the core decay heat.

13.4.5.3.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [11]. The core remains covered during the transient. The lowest RPV water level is 6.1 m, which is higher than the top of the active core (5.724 m). The acceptance criteria are met. After the actuation of two trains of EHR [CHRS], the water temperature in the IRWST is well limited, thus the MHSI pump cavitation is prevented. The containment pressure is maintained below the containment design pressure. In the long term, the decay heat is removed via the EHR [CHRS] and secondary side. The final state of DEC-A is reached, thus the safe state can also be reached.

13.4.5.4 SB-LOCA with Total Loss of LHSI (State C3a/C3b/D)

13.4.5.4.1 Description

SB-LOCA with total loss of LHSI is classified as a DEC-A accident, which is initiated by a small break located at the cold leg. The break size is equivalent diameters no larger than 5.0 cm. The LHSI is assumed to be unavailable.

After the break occurs, the SI signal can be triggered by “RCP [RCS] loop level low 1”. After the MHSI is actuated, the coolant inventory is compensated. The decay heat is transferred into the IRWST. In the long term, the decay heat removal is ensured by the EHR [CHRS].

For short term phase, SB-LOCA with total loss of LHSI in state C3a/C3b/D can be bounded by the DBC-4 event of SB-LOCA in state C1 due to the following reasons:

a) The initial power is higher, which will lead to the larger decay heat generated during the transient.

b) The initial primary pressure is higher, which will lead to the larger mass flow rate at the break and the faster loss of coolant.

c) Only MHSI is used in the short term analysis. There are fewer available MHSI trains than in SB-LOCA with total loss of LHSI.

For long term phase, the analysis of heat removal via EHR [CHRS] can be demonstrated by TLOCC in C3b and D, because the conservative assumption of initial power is the same.

13.4.5.4.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as a target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.4.3 Main Safety Functions

The following safety functions and operator actions are claimed in the analysis of SB-LOCA with total loss of LHSI in state C3a/C3b/D.

a) Automatic protections

“RCP [RCS] loop level low 1” signal triggers the automatic MHSI actuation (FC1).

b) Operator actions

The EHR [CHRS] in spraying mode is manually actuated on the signal of high containment pressure or high water temperature of IRWST. This safety function is a DEC-A feature (FC3).

13.4.5.4.4 Typical Events Sequences

When the SB-LOCA with total loss of LHSI occurs in states C3 and D, the break leads to the loss of coolant. When the “RCP [RCS] loop level low 1” threshold is reached, the actuation of MHSI is triggered to compensate the coolant inventory.

The decay heat is transferred from the core to the containment through the break flow. The EHR [CHRS] in spraying mode is manually actuated to control the containment pressure and temperature. In the long term, the coolant inventory is maintained by the MHSI. The decay heat removal is ensured by the EHR [CHRS].

13.4.5.4.5 Result and Conclusion

For short term phase, SB-LOCA with total loss of LHSI in states C3 and D is bounded by the DBC-4 event of SB-LOCA in state C1, which is described in Reference [12]. For long term phase, the heat removal via EHR [CHRS] is demonstrated in the analysis of TLOCC in C3b and D, which is described in Reference [13].

As a result, the core remains covered during the whole transient. After the actuation of two trains of EHR [CHRS], the water temperature in the IRWST is well limited, thus the MHSI pump cavitation is prevented. The containment pressure is maintained below the containment design pressure. In the long term, the decay heat is removed via the EHR [CHRS]. The final state of DEC-A is reached, thus the safe state can also be reached.

13.4.5.5 Loss of RHR or Failure of Recovery of RHR after LOOP Accident (State C/D)

13.4.5.5.1 Description

Loss of RHR or failure of RHR recovery after LOOP in states C3a/C3b/D are classified as DEC-A accidents, which are initiated by the total loss of RHR. In these

accidents, three RIS [SIS] trains in RHR mode are lost, and the decay heat cannot be removed by RHR.

The loss of three RIS [SIS] trains in RHR mode may be caused by:

a) Failure of LHSI pumps.

b) The malfunction of three trains of RRI [CCWS]/RIS [SIS] heat exchanger.

c) Spurious closure of the valves at the RIS [SIS] point of suction from the hot leg, or of the valves at the point of injection.

d) Spurious RIS [SIS] train isolation signal.

After this accident occurs, if the primary system is open, the SI signal can be triggered by “RCP [RCS] loop level low 1”. After the MHSI is actuated, the coolant inventory is compensated. The decay heat is transferred into the containment and IRWST. In the long term, the decay heat removal is ensured by the EHR [CHRS]. If the primary system is not open, the secondary side can be used to remove the decay heat.

13.4.5.5.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, the above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.5.3 Main Safety Functions

The following safety functions are claimed in the analysis of this accident.

a) Automatic protections

1) VDA [ASDS]

Three trains of VDA [ASDS] open automatically when the SG pressure reaches “SG pressure high 1” to limit the secondary pressure (FC1, for RCP [RCS] pressurisable).

2) ASG [EFWS]

Three trains of ASG [EFWS] are actuated by “SG level (wide range) low 2” signal, and the isolation of ASG [EFWS] is actuated by “SG level (wide range) high 1” signal (FC1, for RCP [RCS] pressurisable).

3) SI signal

“RCP [RCS] loop level low 1” signal triggers the automatic MHSI actuation (FC1, for RCP [RCS] not pressurisable).

b) Operator actions

The EHR [CHRS] in spraying mode is manually actuated on the signal of high containment pressure or high water temperature of IRWST. This safety function is a DEC-A feature (FC3, for RCP [RCS] not pressurisable).

13.4.5.5.4 Typical Events Sequences

When the total loss of RHR occurs in states C3a/C3b/D, if the primary system is open, the coolant keeps evaporating due to decay heat and it may cause core level drop. The SI signal can be triggered by “RCP [RCS] loop level low 1”. Then safety injection can be used to compensate primary coolant inventory. The decay heat is transferred from the core to the containment through evaporation. The EHR [CHRS] in spraying mode is manually actuated to control the containment pressure and temperature. In the long term, the coolant inventory is maintained by the MHSI. The decay heat removal is ensured by the EHR [CHRS].

If the primary system is not open, the secondary side can be used to remove the decay heat.

With the above measures, the long term core cooling can be ensured. Thus the final state is reached.

13.4.5.5.5 Result and Conclusion

If the primary system is open, the total loss of RHR in states C3a/C3b/D is bounded by SB-LOCA with total loss of LHSI in states C3a/C3b/D which has been analysed in Sub-chapter 13.4.5.4 due to the same mitigation measures and the faster loss of coolant of the latter accident.

If the primary system is not open, the secondary side can be used to remove the decay heat. The consequences can be bounded by LUHS (100 hours) in power operation which is analysed in Sub-chapter 13.4.5.14. Because the initial power of the latter accident is higher, it will lead to a larger decay heat which needs to be removed by the secondary side.

13.4.5.6 SBO (State A to F)

SBO (state A to F) in different plant states can be divided into two categories:

1) If the RCP [RCS] is pressurisable, the bounding situation is SBO in state A, in which the decay heat has to be removed through the SGs is the highest.

2) If the RCP [RCS] is not pressurisable, the bounding situation is SBO in state C3b of shutdown condition, in which the decay heat is the highest.

Regarding the SBO accident for SFP, the detailed analysis is provided in Sub-chapter 13.4.5.7.

13.4.5.6.1 SBO (State A)

13.4.5.6.1.1 Description

A SBO accident in state A refers to the LOOP combined with failure of the three Emergency Diesel Generators (EDGs) in state A, which will result in the total loss of normal Alternating Current (AC) power distribution system and emergency AC power distribution system. SBO is an overheating event which can cause fuel and cladding damage. It can also induce the failure of the reactor coolant pump seals resulting in a loss of integrity of the primary system. It belongs to DEC-A sequences.

In this case, the analysis is focused on the reactor coolant pump seals tightness and the continuous residual heat removal by the secondary side. For reactor coolant pump seals tightness, it is required that the temperature and pressure conditions of the final state can meet the safety requirements of the reactor coolant pump seals. For continuous residual heat removal by the secondary side, as long as the SGs water supply is guaranteed, the residual heat from the core can be continuously removed. Therefore the main measures for this event are the control of primary pressure and temperature, and the SGs water supply.

13.4.5.6.1.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as a target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature

shall be maintained at an acceptably low value and decay heat shall be removed.

However, if the core remains covered and the long term core cooling can be ensured during the transient, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.6.1.3 Main Safety Functions

The following safety functions are claimed in the analysis of SBO.

a) Automatic functions

1) RT

The RT is triggered by the “Low RCP [RCS] pump speed” signal (FC1).

2) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

3) VDA [ASDS]

Three trains of VDA [ASDS] open automatically when the SG pressure reaches “SG pressure high 1” to limit the secondary pressure (FC1).

4) PSV

The PSVs automatically open when the opening set-point is reached (FC1).

b) Operator actions

1) Start-up of SBO DGs and start-up of ASG [EFWS]

After SBO detection, two SBO DGs and two ASG [EFWS] pumps in trains A and B are actuated manually from MCR (FC2).

The start-up of SBO DGs and ASG [EFWS] is a key mitigation measure for this accident. It ensures that the residual heat can be continually removed by the secondary side.

2) Opening of the ASG [EFWS] collecting pipe

After start-up of ASG [EFWS], the ASG [EFWS] collecting pipe opening is performed by the operator locally outside the MCR (FC2).

3) Controlled cooling operation

The controlled cooldown is performed { } from the MCR by adjusting the available VDA [ASDS], until the secondary side pressure decreases to { } (FC2).

The controlled cooling operation is a key mitigation measure for this accident. It can prevent the loss of integrity of the primary system due to the failure of the RCP [RCS] seals.

4) SFP cooling

When SG water level is restored and ECS [ECS] is in place, the operator manually switches one train of SBO diesel generator from the ASG [EFWS] to the PTR [FPCTS] to remove the residual heat from SFP (FC2).

13.4.5.6.1.4 Typical Events Sequences

After a SBO accident, if there is no other additional electricity supply (such as SBO DGs), the following main systems will become unavailable:

a) ARE [MFFCS]

b) AAD [SSFS]

c) ASG [EFWS]

d) RCV [CVCS]

e) RIS [SIS]

f) RRI [CCWS]

g) SEC [ESWS]

h) Reactor coolant pump

i) Ventilation system

j) Battery charger

k) PTR [FPCTS]

l) ECS [ECS]

SBO is an overheating DEC-A accident which will cause primary system overpressure. After a SBO accident happens, the three reactor coolant pumps stop working and start to coast down. Then, the “Low RCP [RCS] pump speed” signal will trigger RT for the core protection which will also trigger the turbine trip. With the reactor coolant pump trip and turbine trip, the primary pressure increases and may reach the opening threshold of the PSV.

With the loss of ARE [MFFCS], AAD [SSFS] and ASG [EFWS], the secondary side pressure increases because it is impossible to supply feeding water for all SGs. Consequently, the VDA [ASDS] opens for the overpressure protection of the secondary system. The decay heat is removed by the consumption of SG water and the continuous opening of the VDA [ASDS]. After depletion of the two-hours charge

batteries, the VDA [ASDS] of SG 3 are no longer powered and are isolated. Meanwhile, all Main Steam Isolation Valves (MSIVs) remain open. As a result, the water levels of the SGs decrease constantly. If no effective measures are taken, the SGs will dry out, and the pressure and temperature of primary system will increase rapidly. Meanwhile, the coolant of primary system will be drained away continuously through the opened PSVs, which may lead to fuel and clad damage.

SBO DGs are designed to deal with SBO accidents in the UK HPR1000. After 30 minutes following the RT signal, before the two-hours charge batteries depletion, the SBO DGs are actuated by the operator for the power supply to the ASG [EFWS], VDA [ASDS], ventilation systems, Instrumentation and Control (I&C) systems and other protection systems or relative auxiliary systems. With these measures, the decay heat removal can be implemented; the pressure and temperature of the primary system can be maintained at an appropriate steady-state value to ensure the integrity of the reactor pump seals.

In the long term, three ASG [EFWS] tanks can provide at least 24 hours of water supply for the SGs in state A. When the ASG [EFWS] tanks are drained, they can be refilled from the ASP [SPHRS] tank.

With the above measures, the core remains sub-critical and the long term core cooling can be ensured. Thus the final state is reached.

13.4.5.6.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [14]. The main assumptions are as follows:

a) The accident is assumed to occur at full power state, which is considered to maximise primary heat.

b) Initial reactor power is the nominal power plus the maximum uncertainty (102% FP), which is considered to maximise primary heat, leading to more ASG [EFWS] water consumption.

c) The reactor loop flowrate is the thermal design flowrate, which is considered to penalise heat removal conditions.

d) The RPV coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial pressuriser pressure is the nominal value plus the maximum uncertainty, which is considered to penalise the conditions of RCP [RCS] seals tightness.

f) The initial pressuriser level is the nominal level at power plus 7% based on uncertainties, which is considered to penalise the conditions of RCP [RCS] seals tightness and primary heat.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise water inventory of SGs and the heat removal by secondary side.

h) The core bypass flowrate is maximum, which is considered to penalise heat removal.

i) After the RT, a conservative heat curve (1.645σ uncertainties on the "B+C term") is used for the core decay heat.

13.4.5.6.1.6 Result and Conclusion

The detailed results and conclusions for this accident (see Reference [14]) shows that the core remains covered during the whole process of the accident due to the lowest RPV water level (11.16 m) is higher than the top of the active core (5.724 m). In the long term, the pressure and temperature of the primary system comply with the requirements of reactor pump seals tightness to ensure the primary coolant inventory. The capacity of SBO DGs is sufficient to supply electricity power for 72 hours. The capacity of residual heat removal by the secondary side is always sufficient. Meanwhile, the capacity of ASG [EFWS] and ASP [SPHRS] is sufficient to supply water for all SGs to remove residual heat in the long term. As analysed above, it is concluded that the acceptance criteria are met in SBO accidents in state A.

In addition, as for demonstration of diverse protection line, the capacity of SBO DGs, ASG [EFWS] and ASP [SPHRS] are sufficient to remove residual heat for 24 hours. 24 hours after accident, the offsite electricity supply can be restored, ensuring decay heat removal by the RHR in the long term. The safe state can be reached.

13.4.5.6.2 SBO in Shutdown Condition (State C3b)

13.4.5.6.2.1 Description

SBO in Shutdown Condition refers to the LOOP combined with failure of the three EDGs, which will result in the total loss of normal AC power distribution system and emergency AC power distribution system. The following main systems become unavailable due to the loss of electricity supply:

a) ARE [MFFCS]

b) AAD [SSFS]

c) ASG [EFWS]

d) RCV [CVCS]

e) RIS [SIS]

f) RRI [CCWS]

g) SEC [ESWS]

h) RCP [RCS] pumps

i) Ventilation System

j) Battery Charger

k) PTR [FPCTS]

l) ECS [ECS]

The SBO is classified as a DEC-A accident. The SBO accident in states C3b to F is analysed, which is corresponding to the situations with opened loops. The main potential consequence is the core exposure and heat-up caused by the evaporation of coolant. The situations with closed loops are bounded by the SBO in state A.

In states C3b to F:

a) The RIS [SIS] is running in RHR mode.

b) The primary temperature is between 10 °C and 60 °C.

c) The RCP [RCS] water level is greater than or equal to the lowest level of operation interval of RIS [SIS]/RHR, and less than the level when the reactor pool is filled.

d) All RCP [RCS] pumps are stopped.

e) The RCP [RCS] is at the atmospheric pressure and in open state.

f) The SGs are unavailable to remove the decay heat.

The SBO accident in state C3b is considered as the bounding case for analysis because the decay heat of state C3b is greater than that of other states.

Regarding the SBO accident for SFP, the detailed analysis is provided in Reference [15].

13.4.5.6.2.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as a target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, the above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.6.2.3 Main Safety Functions

The following operator actions are claimed in the analysis of SBO in state C3b.

The SBO diesel generators are manually actuated by the operator to ensure the electrical power supply. This safety function is a DEC-A feature. The following systems will be manually actuated after the start-up of SBO diesel generators:

a) LHSI actuation

The train A and train B of LHSI are manually actuated to maintain the coolant inventory (FC2).

b) Actuation of LHSI pumps diversified cooling chain

The DEL [SCWS] diversified cooling chain is manually actuated to ensure the availability of LHSI pumps (FC2).

c) Actuation of EHR [CHRS]

The EHR [CHRS] in spraying mode is manually actuated on the signal of high containment pressure or high water temperature of IRWST (FC3).

d) Actuation of ECS [ECS]

The ECS [ECS] is manually actuated to provide diversified cooling chain for the EHR [CHRS] (FC3).

13.4.5.6.2.4 Typical Events Sequences

When the SBO in state C3b occurs, the residual heat removal becomes unavailable because of the loss of the RIS [SIS]. The coolant temperature gradually increases to the saturation temperature. After the coolant becomes saturated, the decay heat is removed through the evaporation of the coolant, which leads to the decrease of the RCP [RCS] loop level. After the manual start-up of the SBO diesel generators, trains A and B of LHSI which equip diversified cooling chain is manually actuated to compensate the coolant inventory.

The decay heat is transferred from the core to the containment through evaporation continuously. The EHR [CHRS] in spraying mode is manually actuated to control the containment pressure and temperature. The EHR [CHRS] which equips diversified

cooling supply removes the heat to the Ultimate Heat Sink (UHS) - the ECS [ECS]. In the long term, the coolant inventory is maintained by the LHSI. The decay heat removal is ensured by the EHR [CHRS] and ECS [ECS].

13.4.5.6.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [16]. The main assumptions are as follows:

a) The SBO accident is assumed to occur in state C3b.

b) The RCP [RCS] water level is equal to the lowest level of operation interval of RIS [SIS]/RHR, which is considered to penalise the water inventory.

c) The RPV coolant average temperature is 60 °C, which is considered to maximise the primary heat.

d) The state C3b is reached at least 50.5 hours after the reactor shutdown. It is conservatively assumed that the decay heat is 15.48 MW.

13.4.5.6.2.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [16]. If there is no mitigation measure, the RCP [RCS] water level will decrease to the top of the active core about 119 minutes after the accident. Trains A and B of LHSI are manually actuated to compensate the coolant inventory 60 minutes after the accident. The injection flowrate is much higher than the evaporation rate. The core remains covered during the whole transient. The acceptance criteria are met. After the actuation of two trains of EHR [CHRS], the water temperature in the IRWST is well limited, thus the LHSI pump cavitation is prevented. The containment pressure is maintained below the containment design pressure. In the long term, the decay heat is removed via the EHR [CHRS] and ECS [ECS]. The final state of DEC-A is reached, thus the safe state can also be reached.

13.4.5.7 SBO for Spent Fuel Pool (State A to F)

13.4.5.7.1 Description

This event may cause an inadequate cooling of the fuel assemblies in SFP. The main characteristic of the PTR [FPCTS] is described below.

There are three independent PTR [FPCTS] trains (A/B/C), which have the same capacity, powered by individual electrical switchboards. Each of the three PTR [FPCTS] trains consists of one PTR [FPCTS] pump, one heat exchanger and corresponding lines. When the RRI [CCWS] is available, each heat exchanger can be cooled by RRI [CCWS], otherwise, ECS [ECS] can be used to cool the train A or train B heat exchanger.

Generally, one PTR [FPCTS] train is in operation to remove decay heat from the

Spent Fuel Pool (SFP) during State A to State D, the other two are back up. During State E and State F, two PTR [FPCTS] trains are in operation to remove decay heat from the SFP, the other one is back up.

13.4.5.7.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as a target. The accident should meet the following acceptance criteria:

a) The sub-criticality of the fuel assemblies is ensured.

b) The fuel assemblies in the fuel pool remain covered.

c) The decay heat from the spent fuel pool is removed.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.7.3 Main Safety Functions

After the initial events, the following operator actions are claimed in the analysis of SBO for Spent Fuel Pool:

a) Actuation of emergency diesel generators

The SBO emergency diesel generators are manually actuated to restart ECS [ECS] (FC2).

b) Actuation of PTR [FPCTS]

One train of PTR [FPCTS] cooled by ECS [ECS] is manually actuated to ensure the cooling of SFP (FC2).

13.4.5.7.4 Typical Events Sequences

Generally, one PTR [FPCTS] train is in operation to remove decay heat from the SFP during State A to State D, the other two are back up. During State E and State F, two PTR [FPCTS] trains are in operation to remove decay heat from the SFP, the other one is back up.

After a SBO accident, at initial time, the SFP is cooled by two cooling train (e.g. PTR [FPCTS] trains A and B) and the third PTR [FPCTS] train is stopped, but available.

After the initial events, if the ECS is launched successfully three hours later, one cooling train can be restarted and operate again to maintain the SFP water temperature below the maximum.

The long term SFP cool down is ensured by this PTR [FPCTS] train in operation during the whole transient, in order to maintain the SFP stabilised temperature below the maximum.

13.4.5.7.5 Analysis Assumptions

The detailed assumptions are presented in Reference [15]. The main assumptions are as follows:

a) The spent fuel decay heat in the SFP is considered to be 15.29 MW, considering the uncertainties of 1.645σ, which is the maximum value during all the states.

b) The initial SFP water temperature is considered as 60 °C. This value covers all the states.

c) The initial volume of SFP water is considered as 1265.8 m^3. This volume corresponds to the minimum volume of water inside SFP compartment, when the level is at 16.90 m.

d) A maximal ECS [ECS] inlet temperature is 45 °C.

e) SFP and PTR [FPCTS] pipes are considered as adiabatic.

f) The decay heat which is released from the spent fuel is total absorbed by the water in the SFP.

g) Before the accident, RRI [CCWS] inlet temperature is 45 °C.

h) After SBO, one PTR [FPCTS] cooling train cooled by ECS [ECS] can be loaded in three hours to cool the ECS [ECS].

13.4.5.7.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [15]. The analysis indicates that the fuel assemblies in the fuel pool remain covered during the whole process of the accident. Before the ECS [ECS] is launched successfully, the maximum SFP water temperature (92°C) is lower than the boiling temperature (100°C), so the sub-criticality of the fuel assemblies can be ensured. In the long term, the PTR [FPCTS] is sufficient to maintain the SFP water temperature stable (82.1°C), so the decay heat from the spent fuel pool can be removed. The final state of DEC-A is reached, thus the safe state can also be reached.

13.4.5.8 ATWS Due to RPS [PS] Failure (State A)

13.4.5.8.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods failure to be inserted into the core due to mechanical blockage of rods.

This subsection addresses the ATWS due to the RPS [PS] failure which is postulated

to be caused by software Common Cause Failure (CCF).

In order to mitigate the events mentioned above, the KDS [DAS] has been developed in nuclear power plants. If the software CCF causes the invalidation of the safety functions that are required to cope with the design basis conditions by assumption, the diverse functions provided by KDS [DAS] are performed to mitigate the consequences effectively, Reference [17].

In the following paragraphs, based on international good practice and engineering experience, four typical initiating events listed below are analysed:

a) Loss of Main Feedwater (LOMFW).

b) LOOP.

c) Spurious Pressuriser Spraying.

d) SB-LOCA.

13.4.5.8.2 Acceptance Criteria

13.4.5.8.2.1 Acceptance Criteria for SB-LOCA Combined with ATWS

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, it can be demonstrated that the above criteria are met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.8.2.2 Acceptance Criteria of Non-LOCA Combined with ATWS

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The amount of fuel rods experiencing Departure from Nucleate Boiling (DNB)

must remain less than 10 %.

b) The fuel pellet melting at the hot spot must not exceed 10 % by volume.

c) The peaking cladding temperature must remain less than 1482°C.

If the minimum Departure from Nucleate Boiling Ratio (DNBR) remains above the design limit 1.30 (FC2000 correlation, deterministic method), Reference [18], the criteria are met. The peak pressure of primary loop should remain below 22.37 MPa abs. to ensure the intactness of the primary side.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.8.3 Main Safety Functions

13.4.5.8.3.1 Case 1: LOMFW Combined with ATWS

a) RT

RT is triggered by the “SG level (narrow range) low 1” signal (FC2).

b) Turbine trip

The RT signal automatically triggers the turbine trip (FC2).

c) ASG [EFWS] operation

The “SG level (wide range) low 2” signal starts up the ASG [EFWS] (FC2).

d) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches the “SG pressure high 1” set-point to limit the secondary pressure (FC2).

e) PSV open and closure

The PSVs open and close automatically when the PZR pressure reaches the set-point to limit the primary pressure (FC1).

13.4.5.8.3.2 Case 2: LOOP Combined with ATWS

a) RT

RT is triggered by the “Low flow rate in one primary loop coincident with P8” signal (FC2).

b) ASG [EFWS] operation

The “SG level (wide range) low 2” signal starts up the ASG [EFWS] (FC2).

c) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches the “SG

pressure high 1” set-point to limit the secondary pressure (FC2).

d) PSV open and closure

The PSVs open and close automatically when the PZR pressure reaches the set-point to limit the primary pressure (FC1).

13.4.5.8.3.3 Case 3: Spurious Pressuriser Spraying Combined with ATWS

a) RT

RT is triggered by the “Pressuriser pressure low 2 coincident with P10” signal (FC2).

b) Turbine trip

The RT signal automatically triggers the turbine trip (FC2).

c) ARE [MFFCS] operation

The RT signal triggers the ARE [MFFCS] full load lines of all SGs isolation, and the ARE [MFFCS] low load lines are unavailable (FC2).

d) ASG [EFWS] operation

The “SG level (wide range) low 2” signal starts up the ASG [EFWS] (FC2).

e) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches the “SG pressure high 1” set-point to limit the secondary pressure (FC2).

13.4.5.8.3.4 Case 4: SB-LOCA Combined with ATWS

a) RT

RT is triggered by the “Pressuriser pressure low 2 coincident with P10” signal (FC2).

b) Turbine trip

The RT signal automatically triggers the turbine trip (FC2).

c) ARE [MFFCS] operation

The RT signal triggers the ARE [MFFCS] full load lines of all SGs isolation, and the ARE [MFFCS] low load lines are unavailable (FC2).

d) ASG [EFWS] operation

The “SG level (wide range) low 2” signal starts up the ASG [EFWS] (FC2).

e) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches the “SG pressure high 1” set-point to limit the secondary pressure (FC2).

13.4.5.8.4 Typical Events Sequences

13.4.5.8.4.1 Case 1: LOMFW Combined with ATWS Due to RPS [PS] Failure

The accident is initiated by the loss of all main feedwater pumps and the AAD [SSFS] pumps. The ATWS due to RPS [PS] failure combined with LOMFW is an overheating event resulting in the reduction of the heat removal capability of the SG.

After loss of all feedwater, the SG water inventory decreases continuously. The RT is supposed to be triggered by the “SG level (narrow range) low 1” signal in RPS [PS]. However, because of the software CCF, the RPS [PS] is assumed unavailable during this transient. Under this condition, RT is trigged in the KDS [DAS] by the “SG level (narrow range) low 1” signal. The RT signal automatically triggers the turbine trip.

Afterwards, the secondary pressure increases and is limited by the GCT [TBS] if available. Otherwise, it is limited by the VDA [ASDS]. Once the SG water level reaches the “SG level (wide range) low 2” set-point by the KDS [DAS], the ASG [EFWS] starts to operate automatically to remove the residual decay heat.

Since the decrease of water inventory is in the secondary side, the primary temperature and pressure increase possibly leading to the opening of PSV and the DNBR design limit is challenged. After the RT, the Rod Cluster Control Assemblies (RCCAs) drops into the core and the reactor manages to scram down. In the long term, the VDA [ASDS] and the ASG [EFWS] are performed to remove the decay heat.

13.4.5.8.4.2 Case 2: LOOP Combined with ATWS Due to RPS [PS] Failure

The accident is initiated by the loss of off-site power. The ATWS due to RPS [PS] failure combined with LOOP is an overheating event potentially resulting in DNB and insufficient cooling of the core.

After loss of the power supply, all RCP [RCS] pumps begin to coast down and all feedwater pumps and condensate pumps are tripped.

The coast down of the RCP [RCS] pumps takes several seconds due to the inertia of the flywheel. When the speed of reactor coolant pump reaches the “low RCP [RCS] pump speed” set-point, the RT is supposed to be trigged. However, because of the software CCF, the RPS [PS] is assumed unavailable during the transient. Under this condition, the RT is trigged in the KDS [DAS] by the “Low flow rate in one primary loop coincident with P8” signal.

Since the turbine and feedwater pumps are tripped, the heat removal capacity of the SGs decreases and the SG pressure increases continuously. The GCT [TBS] is unavailable during this transient on account of the loss of condensate pumps. The VDA [ASDS] is actuated to limit the secondary pressure. Once the SG water level reaches the “SG level (wide range) low 2” set-point, the ASG [EFWS] is actuated by KDS [DAS] to remove the residual decay heat.

With coasting down of RCP [RCS] pumps, the heat removal capacity of the primary loop decreases because of the reduction of reactor coolant flow rate. This results in the augmentation of primary temperature and pressure and the DNBR design limit is challenged. After the RT, RCCAs drop into the core and the reactor manages to scram down. In the long term, the VDA [ASDS] and the ASG [EFWS] are performed to remove the decay heat.

13.4.5.8.4.3 Case 3: Spurious Pressuriser Spraying Combined with ATWS Due to RPS [PS] Failure

The accident is initiated by the spurious pressuriser spraying. The ATWS due to RPS [PS] failure combined with the spurious pressuriser spraying is an overheating event potentially resulting in the DNB and the pressure drop of the primary loop.

After the spurious pressuriser spraying, the RCP [RCS] pressure decreases. The RT is supposed to be triggered by the “Pressuriser pressure low 2” signal. However, because of the software CCF, the RPS [PS] is assumed unavailable during this transient. Under this condition, the RT is trigged in the KDS [DAS] by the “Pressuriser pressure low 2 coincident with P10” signal.

After RT, the RCCAs drop into the core and the reactor manages to scram down. The turbine trips automatically. After that, the ARE [MFFCS] full load lines isolation valves are automatically closed. Afterwards, the secondary pressure increases and is limited by the GCT [TBS] if available. Otherwise, it is limited by the VDA [ASDS]. When SG level decreases to the “SG level (wide range) low 2” signal, the ASG [EFWS] is started up by KDS [DAS] to supply water to the SGs automatically.

The spurious pressuriser spraying leads to the primary pressure decrease. Consequently, the DNBR design limit is challenged. In the long term, the VDA [ASDS] and the ASG [EFWS] are performed to remove the decay heat.

13.4.5.8.4.4 Case 4: SB-LOCA Combined with ATWS Due to RPS [PS] Failure

A small break located at the cold leg will lead to a decrease of the coolant inventory, which cannot be compensated by the RCV [CVCS]. The break area is assumed as 20 cm^2.

The loss of primary coolant leads to a decrease of the RCP [RCS] pressure and the water level in the PZR. The RT is supposed to be triggered by the “Pressuriser pressure low 2 coincident with P10” signal. However, because of the software CCF, the RPS [PS] is assumed unavailable during the transient. In this condition, the RT is trigged in the KDS [DAS] by the “Pressuriser pressure low 2 coincident with P10” signal.

Then the turbine trip occurs and the ARE [MFFCS] full load lines isolation valves are closed coincidently with the RT. In the analysis of this accident, it is assumed conservatively that the low load lines of the ARE [MFFCS] are unavailable and the

ASG [EFWS] is used to control the SG water level. The SG pressure increases rapidly to the "SG pressure high 1" threshold after the turbine trip, the VDA [ASDS] opens automatically to prevent the overpressure of the secondary side.

When the primary pressure decreases to the "Pressuriser pressure low 3" threshold, the SI signal is triggered. The RCP [RCS] pumps will stop due to the combination of the SI signal and "RCP [RCS] pump ΔP low 1" signal. The SI signal also triggers the MCD. The MCD cools down the primary system with a cooling rate of 250 °C/h. During the MCD, the MHSI injection pressure is reached and the coolant inventory is compensated by the MHSI. The RPV water level starts to recover.

The MCD ends when the SG pressure decreases to 6.0 MPa. The primary pressure is still too high for the accumulators or LHSI to inject. Manual actions are performed by the operator to mitigate the accident. Two RBS [EBS] pumps are manually actuated to inject borated water into the RCP [RCS]. Three trains of VDA [ASDS] are manually adjusted to cool the primary system { }. The decay heat is continuously removed through the secondary system. The pressure and temperature of the primary system decrease during the controlled cooling operation. The accumulator starts to inject water into the RCP [RCS] as soon as the injection pressure is reached.

In this analysis, the final state of DEC-A is reached after the RHR is connected.

13.4.5.8.5 Analysis Assumptions

13.4.5.8.5.1 Case 1: LOMFW Combined with ATWS

The detailed assumptions are presented in Reference [19]. The main assumptions are as follows:

13.4.5.8.5.1.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty, which is considered to maximise primary heat.

b) The initial coolant flowrate is the thermal design flowrate, which is considered to penalise the heat removal.

c) The core bypass flowrate is maximised to penalise the heat removal.

d) The average temperature of the coolant is the nominal value plus the maximum uncertainty, which is considered to maximise the primary heat.

e) The initial pressure of the pressuriser is the nominal value minus the maximum uncertainty so as to penalise the DNBR.

f) The initial pressuriser level is the nominal level minus the maximum uncertainty, which is considered to penalise the DNBR.

13.4.5.8.5.1.2 Core-related Assumptions

The neutronic data are considered as follows:

a) The moderator density coefficient is considered as its minimum value.

b) The Doppler power coefficient is considered as its maximum value (in absolute value).

c) The Doppler temperature coefficient is considered as its maximum value.

All the RCCAs are assumed to be inserted in the core after RT and the most conservative negative reactivity insertion curve as a function of time is used.

13.4.5.8.5.2 Case 2: LOOP Combined with ATWS

The detailed assumptions are presented in Reference [19]. The main assumptions are as follows:

13.4.5.8.5.2.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty, which is considered to maximise primary heat.

b) The initial coolant flowrate is the thermal design flowrate, which is considered to penalise the heat removal.

c) The core bypass flowrate is the maximum to penalise the heat removal.

d) The average temperature of the coolant is the nominal value plus the maximum uncertainty, which is considered to maximise the primary heat.

e) The initial pressure of the pressuriser is the nominal value minus the maximum uncertainty so as to penalise the DNBR.

f) The initial pressuriser level is the nominal level minus the maximum uncertainty, which is considered to penalise the DNBR.

13.4.5.8.5.2.2 Core-related Assumptions

The neutronic data are considered as follows:

a) The moderator density coefficient is considered as its minimum value.

b) The Doppler power coefficient is considered as its maximum value (in absolute value).

c) The Doppler temperature coefficient is considered as its maximum value.

All the RCCAs are assumed to be inserted in the core and the most conservative negative reactivity insertion curve as a function of time is used.

13.4.5.8.5.3 Case 3: Spurious Pressuriser Spraying Combined with ATWS

The detailed assumptions are presented in Reference [19]. The main assumptions are as follows:

13.4.5.8.5.3.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty, which is considered to maximise primary heat.

b) The initial coolant flowrate is the thermal design flowrate, which is considered to penalise the heat removal.

c) The core bypass flowrate is the maximum to penalise the heat removal.

d) The average temperature of the coolant is the rated value plus the maximum uncertainty, which is considered to maximise the primary heat.

e) The initial pressure of the pressuriser is the rated value minus the maximum uncertainty, which is considered to penalise the DNBR.

f) The initial pressuriser level is the rated value minus the maximum uncertainty, which is considered to penalise the DNBR.

13.4.5.8.5.3.2 Core-related Assumptions

The neutronic data are considered as follows:

a) The moderator density coefficient is considered as its minimum value.

b) The Doppler power coefficient is considered as its maximum value (in absolute value).

c) The Doppler temperature coefficient is considered as its maximum value.

All the RCCAs are assumed to be inserted in the core and the most conservative negative reactivity insertion curve as a function of time is used.

13.4.5.8.5.4 Case 4: SB-LOCA Combined with ATWS

The break is located at the cold leg. A break with an equivalent area 20 cm^2 is considered. The detailed assumptions are presented in Reference [19]. The main assumptions are as follows:

13.4.5.8.5.4.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty, which is considered to maximise the primary heat.

b) The reactor loop flowrate is the thermal design flowrate, which is considered to penalise the heat removal.

c) The RPV coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise the primary heat.

d) The initial pressuriser pressure is the nominal value plus the maximum uncertainty, which is considered to delay the RT and SI signal.

e) The initial pressuriser level is the nominal level at power minus the maximum uncertainty based on uncertainties, which is considered to penalise the water inventory of the primary system.

f) The initial SG level is the nominal level at power minus the maximum uncertainty based on uncertainties, which is considered to penalise the water inventory of the secondary system.

g) The core bypass flowrate is maximum, which is considered to penalise the heat removal.

13.4.5.8.5.4.2 Decay Heat Assumption

The decay heat is considered with an uncertainty of 2σ on the “B+C term”.

13.4.5.8.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [19].

a) In the analysis of LOMFW combined with ATWS due to RPS [PS] failure, the minimum DNBR is 2.08, which is above the design limit 1.30 (FC2000 correlation, deterministic method). The peak pressure of primary loop reaches 17.09 MPa below the 130% design pressure (22.37 MPa abs.). It is concluded that the acceptance criteria are met. In the long term, the decay heat is removed by the operation of the VDA [ASDS] and ASG [EFWS], which ensures the RIS [SIS] connection condition in RHR mode is met, the reactor heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

b) In the analysis of LOOP combined with ATWS due to RPS [PS] failure, the minimum DNBR is 1.50, which is above the design limit 1.30 (FC2000 correlation, deterministic method). The peak pressure of primary loop reaches 17.2 MPa below the 130% design pressure (22.37 MPa abs.). It is concluded that the acceptance criteria are met. In the long term, the decay heat is removed by the operation of the VDA [ASDS] and ASG [EFWS], which ensures the RIS [SIS] connection condition in RHR mode is met, the reactor heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

c) In the analysis of spurious pressuriser spraying combined with ATWS due to RPS [PS] failure, the minimum DNBR is 1.90, which is above the design limit 1.30 (FC2000 correlation, deterministic method). The primary pressure continues to

drop, which is always below the 130% design pressure (22.37 MPa abs.). It is concluded that the acceptance criteria are met. In the long term, the decay heat is removed by the operation of the VDA [ASDS] and ASG [EFWS], which ensures the RIS [SIS] connection condition in RHR mode is met, the reactor heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

d) In the SB-LOCA combined with ATWS due to RPS [PS] failure analysis, no core uncover occurs. The manual cooldown operation is capable of the RCP [RCS] depressurisation and the MHSI and LHSI injection flow could sufficiently compensate the coolant inventory during the transient. In the long term, the decay heat removal is ensured by the RHR. It is concluded that the acceptance criteria are met in this accident. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.9 ATWS due to Failure of RCCA to Insert (State A)

13.4.5.9.1 ATWS-Loss of Main Feedwater

13.4.5.9.1.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods failure to be inserted into the core due to mechanical blockage of rods.

The loss of main feedwater - ATWS transient caused by mechanical blockage of rods is analysed in this subsection, while ATWS due to protection system failure will be analysed in other subsection.

In an ATWS accident with loss of main feedwater, the reduction of feedwater flow rate leads to the inventory decrease of the SGs which triggers “SG level (narrow range) low 1” signal. The “SG level (narrow range) low 1” signal will result in reactor trip. However, the reactor does not scram as the RCCAs fail to insert.

This accident leads to a significant increase of the primary pressure and temperature, which challenges the primary pressure boundary most. The main mitigation measures for this event are the PSV opening and the RBS [EBS] injection.

13.4.5.9.1.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The number of fuel rods experiencing DNB must remain below than 10 %.

b) The fuel pellet melting at the hot spot must not exceed 10 % by volume.

c) The peaking cladding temperature must remain less than 1482 °C.

For this accident, if the minimum DNBR remains above the design limit 1.30 (FC2000 correlation, deterministic method) [18], the criteria are met. The peak pressure of primary loop should remain below 22.37 MPa abs. to ensure the intactness of the primary side.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.9.1.3 Main Safety Functions

The safety functions used to cope with this accident are introduced as follows:

a) RT

The “SG level (narrow range) low 1” signal triggers the reactor trip (FC1).

b) “ATWS” signal

The high rod position combined with RT signal triggers of the “ATWS” signal (FC2).

c) Turbine trip

The RT signal triggers the turbine trip (FC1).

d) The third group valves of the GCT [TBS] close.

The RT signal triggers the third group valves of the GCT [TBS] to close (FC3).

e) The forth group valves of the GCT [TBS] close.

The RT signal delay 50 s triggers the forth group valves of the GCT [TBS] to close (FC3).

f) RCP [RCS] pumps stop

The “SG level (narrow range) low 1” signal combined with the “ATWS” signal triggers the pumps to stop (FC2).

g) ASG [EFWS] operation

The ASG [EFWS] is activated by the “SG level (wide range) low 2” signal (FC1).

h) PSVs opening and closure

The PSVs open and close automatically to limit the primary pressure when the pressure reaches the set-point. The PSV operation is a key mitigation measure for this accident, because it can maintain the primary pressure within the acceptance criteria (FC1).

i) VDA [ASDS] open and close

The VDA [ASDS] open and close automatically to limit the secondary pressure when the pressure reaches the set-point (FC1).

j) MSIV closure

The automatic MSIVs isolation is triggered by the “Pressure drop of SG high 1” signal or the “SG pressure low 1” signal (FC1).

k) RBS [EBS] operation

The “ATWS” signal initiates the RBS [EBS] operation automatically. The RBS [EBS], part of the DEC-A features, is one of the key systems to mitigate this accident (FC2).

13.4.5.9.1.4 Typical Events Sequences

In an ATWS accident initiated by loss of main feedwater, the reduction of feedwater flow rate leads to the decrease of the SGs inventory which triggers “SG level (narrow range) low 1” signal. This signal then results in the RT and the turbine trip. However, the reactor does not shutdown as the RCCAs fail to insert. This accident leads to a significant increase of the primary pressure and temperature at the early stage, which challenges the primary pressure boundary most.

Since the decrease of water inventory in the secondary side due to loss of main feedwater, the primary temperature and pressure increase. Once it is detected that the rods are still at high positions after the occurrence of the RT signal, the “ATWS” signal is triggered. The “ATWS” signal initiates the RBS [EBS] automatically. The RCP [RCS] pumps are tripped on “ATWS” signal combined with the “SG level (narrow range) low 1” signal.

After the turbine trips, the steam is discharged either by GCT [TBS] or VDA [ASDS]. The SG water level decreases sharply leading to the decrease of heat removal capability of the secondary side. This leads to a significant increase in the primary pressure and temperature which results in the opening of PSVs. After the RCP [RCS] pumps stopped, the primary coolant flow rate decreases rapidly. Loss of forced circulation leads to the decrease of heat transfer from the primary side to the secondary side. The primary temperature rises drastically. The core power decreases due to the negative feedback effect of the reactor coolant, thus slowing down the increase rate of the primary pressure and temperature.

The “SG level (wide range) low 2” signal activates the ASG [EFWS]. The SGs water inventory is recovered by the ASG [EFWS] gradually. The primary temperature and pressure still increase before the recovery. The “SG pressure low 1” signal initiates the MSIVs automatically.

In the long term, the residual heat is removed by the VDA [ASDS] of all SGs with feedwater supplied by the ASG [EFWS], meanwhile the RBS [EBS] boron injection

ensures that the core remains subcritical. The final state of DEC-A is reached after the RHR is connected.

13.4.5.9.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [20]. The main assumptions are as follows:

13.4.5.9.1.5.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty to maximise the primary heat.

b) The initial reactor coolant flowrate is set as the thermal design flow, considering that 10 % of the SGs tubes are plugged.

c) The primary temperature is the rated value plus the maximum uncertainty to penalise the primary pressure.

d) The primary pressure is the rated value plus the maximum uncertainty to penalise the primary pressure.

e) The initial PZR level is the rated value plus the maximum uncertainty to penalise the primary pressure.

13.4.5.9.1.5.2 Core-related Assumptions

The neutronic data are considered as follows:

a) The moderator temperature coefficient is adopted, which envelopes 99% of the whole nuclear plant life time.

b) The Doppler power coefficient is adopted as the same condition of the moderator temperature coefficient.

c) The Doppler temperature coefficient is adopted as the same condition of the moderator temperature coefficient.

13.4.5.9.1.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [20].The minimum DNBR in the loss of main feedwater - ATWS accident is 2.07 greater than the limit 1.30 (FC2000 correlation, deterministic method). In the meantime, the peak primary pressure is 21.5 MPa, which does not exceed the maximum allowable pressure of 22.37 MPa abs. Therefore, the integrity of the RCP [RCS] is not challenged during the process of this accident. It is concluded that the acceptance criteria are met.

In the long term, the residual heat is removed by the VDA [ASDS] of all SGs with the feedwater supplied by the ASG [EFWS]. The RBS [EBS] boron injection ensures that

the core remains subcritical. The final state of DEC-A is reached after the RHR is connected. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.9.2 ATWS by Rods Failure -Loss of Offsite Power

13.4.5.9.2.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods fail to be inserted into the core due to mechanical blockage of rods.

The LOOP - ATWS transient caused by mechanical blockage of rods is analysed in this report. LOOP will lead to loss of power for all auxiliary plant equipment, such as RCP [RCS] pumps, condensate and main feedwater pumps, etc. It is an overheating event combined with trip of RCP [RCS] pumps potentially, which results in DNB and insufficient cooling of the core.

13.4.5.9.2.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The number of fuel rods experiencing DNB must remain below than 10 %.

b) The fuel pellet melting at the hot spot must not exceed 10 % by volume.

c) The peaking cladding temperature must remain less than 1482 °C.

If the minimum DNBR remains above the design limit 1.30 (FC2000 correlation, deterministic method) [18], the criteria are met. The peak pressure of primary loop should remain below 22.37 MPa abs. to ensure the intactness of the primary side.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.9.2.3 Main Safety Functions

The following paragraphs present the main safety functions applied in ATWS caused by mechanical blockage combined with LOOP.

a) RT signal

The RT signal is triggered by the “Low RCP [RCS] pump speed” (FC1).

b) ATWS signal

The high rod position combined with RT signal triggers the ATWS signal (FC2).

c) Turbine trip

The RT signal triggers the turbine trip (FC1).

d) ASG [EFWS] operation

The “SG level (wide range) low 2” signal starts up the ASG [EFWS] (FC1).

e) PSV opening and closure

The PSVs open and close automatically when the pressure reaches the setpoint to limit the primary pressure (FC1).

f) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1” setpoint to limit the secondary pressure (FC1).

g) RBS [EBS] operation

The ATWS signal starts up the RBS [EBS] operation automatically. The automatic start-up of RBS [EBS] is one of key functions to mitigate the accident, which belongs to the DEC-A features (FC2).

13.4.5.9.2.4 Typical Events Sequences

LOOP will lead to loss of power for all auxiliary plant equipment, such as RCP [RCS] pumps, condensate pumps and main feedwater pumps.

After LOOP, RCP [RCS] pumps coast down and coolant flow rate decreases. The RT signal is emitted on “Low RCP [RCS] pump speed” signal. However, although the RT signal has been emitted, the control rods are still at high positions due to mechanical blockage. Therefore, the reactor trip is not realised. The coolant flow rate decreases and temperature rises. It may lead to a decrease in the DNBR margin. Finally, the core is cooled through natural circulation flow. In this accident, the DNBR design limit is the greatest challenge.

The high rod position combined with RT signal leads to the triggering of the “ATWS” signal which starts up the RBS [EBS] operation.

The opening of the PSVs limits the primary pressure rise, and the VDA [ASDS] ensures the removal of the secondary heat and limits the secondary pressure. When the SG level decreases to the “low SG level (wide range) low 2”, the ASG [EFWS] is started up to supply water to the SG. ASG [EFWS] and RBS [EBS] pumps are started up according to the EDG reloading sequence following LOOP.

13.4.5.9.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [21]. The main assumptions are as follows:

13.4.5.9.2.5.1.1 Initial Conditions

a) Initial reactor power is maximised, which is considered to maximise primary heat.

b) The thermal design flowrate is considered to penalise heat removal.

c) The primary temperature is maximised to minimise the DNBR.

d) The primary pressure is minimised to minimise the DNBR.

e) The initial pressuriser level is minimised to minimise the DNBR.

f) The core bypass flowrate is maximum, which is considered to penalise heat removal.

13.4.5.9.2.5.1.2 Core-related Assumptions

a) The moderator temperature coefficient is adopted, which envelopes above 99% of the whole nuclear plant life time.

b) The Doppler temperature coefficient is adopted at the same condition of the moderator temperature coefficient.

c) The Doppler power coefficient is adopted at the same condition of the moderator temperature coefficient.

13.4.5.9.2.6 Results and Conclusions

The detailed assumptions are presented in Reference [21].

The analysis shows the peak primary pressure is 18.98 MPa abs., which does not exceed the 130% design pressure (22.37 MPa abs.). The DNBR reaches its minimum value 1.40, which is above the design limit 1.30 (FC2000 correlation, deterministic method). It is concluded that the acceptance criteria are met. The inherent safety of the nuclear plant ensures the acceptance criteria concerning DNBR are satisfied. The opening of the PSV limits the primary pressure to guarantee the intact of primary side. The reactor heat is removed by the VDA [ASDS] and ASG [EFWS] in the long term and the final state and safety state can be reached by the cooldown of the secondary side.

13.4.5.9.3 ATWS by Rods Failure - Small Break - Loss of Coolant Accident (SB-LOCA) (State A)

13.4.5.9.3.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods fail to be inserted into the core due to mechanical blockage of rods.

SB-LOCA is defined as a break with an equivalent diameter smaller than or equal to 5.0 cm occurring on the RCP [RCS] line. ATWS transients caused by mechanical blockage of rods following an SB-LOCA are analysed in this report.

In the SB-LOCA combined with ATWS, the primary coolant leaks to the containment which causes the reduction of primary coolant inventory and PZR pressure. In addition, because of the mechanical blockage, RCCAs cannot be inserted. The RCP [RCS] water level and Peaking Cladding Temperature (PCT) are two of the greatest challenges in the transient.

13.4.5.9.3.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, it can be demonstrated that the above criteria are met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.9.3.3 Main Safety Functions

The following paragraphs present the main safety functions applied in ATWS caused by mechanical blockage combined with SB-LOCA.

a) RT Signal

The RT signal is triggered by the “PZR pressure low 2” (FC1).

b) ATWS signal

The high rod position combined with RT signal triggers the ATWS signal (FC2).

c) Turbine trip

The RT signal triggers the turbine trip (FC1).

d) Main feedwater full load line isolation

Main feedwater full load lines of all SGs are isolated on RT signal (FC1).

e) SI signal

The SI signal is triggered by the “PZR pressure low 3” signal (FC1).

f) MCD

The MCD is triggered by the SI signal (FC1).

g) ASG [EFWS] operation

The ASG [EFWS] is started up by the “SG level (wide range) low 2” signal (FC1).

h) PSV open and closure

The PSVs open and close automatically when the PZR pressure reaches the setpoint to limit the primary pressure (FC1).

i) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1” setpoint to limit the secondary pressure (FC1).

j) RBS [EBS] operation

The ATWS signal starts up the RBS [EBS] operation automatically. The automatic start-up of RBS [EBS] is one of key functions to mitigate the accident, which belongs to the DEC-A features (FC2).

k) RCP [RCS] pumps trip

The RCP [RCS] pumps are tripped on ATWS signal combined with the “SG level (narrow range) low 1” signal (FC2).

l) MSSV

The MSSVs open and close automatically when the SG pressure reaches the setpoint to limit the secondary pressure (FC1).

m) Operator actions

Some operator actions are performed to reach the final state. The operator will manually open three trains of VDA [ASDS] to cool down the primary system and stop the MHSI so that the accumulators and LHSI could perform injection (FC2).

13.4.5.9.3.4 Typical Events Sequences

In the SB-LOCA combined with ATWS, the break is supposed to be located in the cold leg of the RCP [RCS]. The reduction of primary coolant leads to a decrease in the RCP [RCS] pressure and the PZR water level which cannot be compensated by RCV [CVCS]. The “PZR pressure low 2” signal triggers the RT signal, which automatically trips the turbine and isolates the full load lines of the ARE [MFFCS]. The SGs are fed with water by the ARE [MFFCS] system through the low load lines. If the low load lines of the ARE [MFFCS] are unavailable, the ASG [EFWS] is used to control the SG level while SG water level decrease to the “SG level (wide range) low 2” signal. After isolation of full load line of ARE [MFFCS], the secondary side heat removal capacity decreases so that the VDA [ASDS] and MSSV open automatically to limit the secondary pressure when SG pressure reaches corresponding set point.

However, due to failure of RCCAs, the control rods cannot be inserted. Once it is detected that the rods are still at high positions combined with RT signal, the ATWS signal is triggered. The ATWS signal starts up the RBS [EBS] automatically. The RCP [RCS] pumps are tripped on ATWS signal combined with the “SG level (narrow range) low 1” signal. In the short term, the decrease in reactor power is induced by the moderator temperature feedback and Doppler temperature feedback. In long term, sub-criticality of the core is provided by boron injection of RBS [EBS].

The “PZR pressure low 3” signal triggers the SI signal. The SI signal starts up MHSI pumps automatically and triggers MCD with a cooling rate of 250 °C/h at the same time. The MCD cools down the primary system and reduces the RCP [RCS] pressure. When the MCD ends, the primary pressure is still too high for the accumulators or LHSI to perform injection. Therefore, 30 minutes after the first significant signal (such as RT signal), the operator will manually open the VDA [ASDS] to cool down the primary system { }.

13.4.5.9.3.5 Analysis Assumptions

For this analysis, a break with an equivalent diameter 2.5 cm and 5.0 cm are taken into consideration. Apart from the break size, the analysis assumptions introduced in the following chapters are identical in the two transients.

The detailed assumptions are presented in Reference [22]. The main assumptions are as follows:

13.4.5.9.3.5.1.1 Initial Conditions

a) Initial reactor power is maximised, which is considered to maximise primary heat.

b) The thermal design flowrate is considered to penalise heat removal.

c) The primary temperature is maximised to maximise primary heat.

d) The primary pressure is maximised to delay the RT and SI signals.

e) The initial pressuriser level is minimised to penalise RCP [RCS] water inventory.

f) The core bypass flowrate is maximum, which is considered to penalise heat removal.

g) The initial SG water level is minimised to penalise the heat removal by secondary side.

13.4.5.9.3.5.1.2 Core-related Assumptions

a) The maximum moderator temperature coefficient is adopted, which envelopes 100% of the whole nuclear plant life time.

b) The Doppler temperature coefficient is adopted at the same condition of the moderator temperature coefficient.

13.4.5.9.3.6 Results and Conclusions

The detailed assumptions are presented in Reference [22].

During the whole transient, for the break with an equivalent diameter 2.5 cm, the lowest RPV water level (7.7 m) is above the top of the active core (5.724 m). For the break with an equivalent diameter 5.0 cm, the lowest RPV water level (6.2 m) is above the top of the active core (5.724 m). It is concluded that the acceptance criteria are met. The inherent safety of nuclear plant ensures the acceptance criteria are satisfied. The injection of the SI compensates the coolant inventory to guarantee the core covered. The reactor heat is removed by the VDA [ASDS] and ASG [EFWS], which ensures the RIS [SIS] connection condition in RHR mode is met, the reactor heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.9.4 ATWS by Rods Failure - Spurious Pressuriser Spraying (State A)

13.4.5.9.4.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods failure to be inserted into the core due to mechanical blockage of rods.

The spurious pressuriser spraying - ATWS transient caused by mechanical blockage of rods is analysed in this subsection.

This event can be caused by:

a) Spurious opening of a normal spray control valve.

b) Spurious opening of an auxiliary spray control valve.

c) An automatic pressure control malfunction.

d) Spurious operator action.

The cause of this event is the spurious opening of two normal spray control valves. It is an envelope case among all the possible causes of spurious pressuriser spraying.

The spurious pressuriser spraying induces a pressure decrease of the primary circuit, which results in RT and turbine trip. However, the reactor does not shutdown as the RCCAs fail to insert.

This accident leads to a significant increase in the primary pressure and temperature, which challenges the primary pressure most. In the short term, the PSV limits the primary pressure to rise. In the long term, the RBS [EBS] boron injection ensures that the core remains subcritical.

13.4.5.9.4.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The number of fuel rods experiencing DNB must remain below than 10 %.

b) The fuel pellet melting at the hot spot must not exceed 10 % by volume.

c) The peaking cladding temperature must remain less than 1482 °C.

For this accident, if the minimum DNBR remains above the design limit 1.30 (FC2000 correlation, deterministic method) [18], the criteria are met. Besides, the peak pressure of primary loop should remain below 22.37 MPa abs. to ensure the intactness of the primary side.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.9.4.3 Main Safety Functions

The safety functions used to cope with this accident are introduced as follows.

a) RT

The “Pressuriser pressure low 2” signal triggers the reactor trip (FC1).

b) “ATWS” signal

The high rod position combined with RT signal triggers of the “ATWS” signal (FC2).

c) Turbine trip

The RT signal triggers the turbine trip (FC1).

d) The third group valves of the GCT [TBS] close

The RT signal triggers the third group valves of the GCT [TBS] close (FC3).

e) The forth group valves of the GCT [TBS] close

The RT signal delay 50 s triggers the forth group valves of the GCT [TBS] close (FC3).

f) RCP [RCS] pumps stop

The “SG level (narrow range) low 1” signal combined with the “ATWS” signal triggers the pumps to stop (FC2).

g) ARE [MFFCS] operation

The RT signal triggers the ARE [MFFCS] full load lines of the SGs isolation automatically. The SGs are fed with water by the ARE [MFFCS] system through the low load lines (FC1).

h) ASG [EFWS] operation

The ASG [EFWS] is activated by the “SG level (wide range) low 2” signal (FC1).

i) PSVs open and closure

The PSVs open and close automatically to limit the primary pressure when the pressure reaches the set-point. The PSVs operation is a key mitigation measure for this accident, because it can maintain the primary pressure within the acceptance criterion (FC1).

j) VDA [ASDS] open and close

The VDA [ASDS] open and close automatically to limit the secondary pressure when the pressure reaches the set-point (FC1).

k) MSIV closure

The automatic MSIVs isolation is triggered by the “Pressure drop of SG high 1” signal or the “SG pressure low 1” signal (FC1).

l) RBS [EBS] operation

The “ATWS” signal initiates the RBS [EBS] operation automatically. The RBS [EBS], part of the DEC-A features, is one of the key systems to mitigate this accident (FC2).

13.4.5.9.4.4 Typical Events Sequences

The spurious pressuriser spraying induces a pressure decrease on the primary circuit. RT is triggered by the “Pressuriser pressure low 2” signal. However, although the RT

signal has been emitted, the control rods are still at high positions due to mechanical blockage. Therefore, the reactor trip is not realised.

Then the turbine trips automatically. After that, the ARE [MFFCS] full load lines are automatically closed, and the SGs are fed with water by the ARE [MFFCS] system through the low load lines. The RT signal also triggers the third group valves of the GCT [TBS] to close automatically and after 50s the fourth group valves to close automatically.

The high rod position combined with RT signal leads to the triggering of the “ATWS” signal which initiates the RBS [EBS] operation.

The opening of the PSVs limits the primary pressure rise. The GCT [TBS] and the VDA [ASDS] ensure the removal of the secondary heat. When the SG level decreases to the “SG level (narrow range) low 1”, combined with the ATWS signal, the reactor coolant pumps stop automatically which causes the spray losing its pressure head, then the spurious spraying ends. When SG level decreases to the “SG level (wide range) low 2”, the ASG [EFWS] is started up to supply water to the SG automatically. The “SG pressure low 1” signal initiates the MSIVs closure automatically, the GCT [TBS] is isolated.

In the final state, the residual heat is removed by the VDA [ASDS] of all steam generators, the feedwater is supplied by the ASG [EFWS], and the RBS [EBS] boron injection ensures that the core remains subcritical in the long term.

13.4.5.9.4.5 Analysis Assumptions

The detailed assumptions are presented in Reference [23]. The main assumptions are as follows:

13.4.5.9.4.5.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty to maximise the primary heat.

b) The initial reactor coolant flowrate is set as the thermal design flow, considering that 10 % of the SGs tubes are plugged.

c) The primary temperature is the rated value plus the maximum uncertainty to penalise the primary pressure.

d) The primary pressure is the rated value plus the maximum uncertainty to penalize the primary pressure.

e) The initial PZR level is the rated value plus the maximum uncertainty to penalise the primary pressure.

13.4.5.9.4.5.2 Core-related Assumptions

The neutronic data are considered as follows:

a) The moderator temperature coefficient, is set at its minimum value (in absolute value) at the beginning of the transient, which envelopes 100 % of the whole nuclear plant life time.

b) The Doppler power coefficient, which tends to limit the nuclear power decrease, is set at its maximum value (in absolute value).

c) The Doppler temperature coefficient, which induces a nuclear power decrease when the coolant temperature increases, is set at its minimum value (in absolute value).

13.4.5.9.4.6 Results and Conclusions

The detailed assumptions are presented in Reference [23].

The minimum DNBR in the spurious pressuriser spraying - ATWS accident is 1.98 greater than the limit 1.30 (FC2000 correlation, deterministic method). In the meantime, the peak primary pressure is 18.0 MPa abs., which does not exceed the maximum allowable pressure of 22.37 MPa abs. Therefore, the integrity of the RCP [RCS] is not challenged during the process of this accident. It is concluded that the acceptance criteria are met.

In the long term, the residual heat is removed by the VDA [ASDS] of all SGs with the feedwater supplied by the ASG [EFWS]. The RBS [EBS] boron injection ensures that the core remains subcritical. The final state of DEC-A is reached after the RHR is connected. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.9.5 ATWS by Rods Failure - Excessive Increase in Secondary Steam Flow (State A)

13.4.5.9.5.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods failure to be inserted into the core due to mechanical blockage of rods.

The excessive increase in secondary steam flow - ATWS transient caused by mechanical blockage of rods is analysed in this subsection.

The excessive increase in secondary system steam flow may be caused by the following reasons:

a) A spurious opening of GCT [TBS] control valves.

b) A spurious actuation of ASP [SPHRS].

c) An excessive opening of turbine inlet valves.

The excessive increase in secondary system steam flow (excessive load increase incident) is defined as a 10% step load increasing in the steam flow that causes a power mismatch between reactor power and steam flow demand, which results in RT and turbine trip. However, the reactor does not shutdown as the RCCAs fail to insert.

This accident may thus lead to an inadequate cooling of the fuel cladding by DNB. The consequences of the event are considered in the plant design and can be managed with meeting the proper acceptance criteria. This accident challenges the DNBR limit most.

In the short term, the negative moderator temperature feedback and negative Doppler temperature feedback lead to the nuclear power decreasing to limit DNBR. In the long term, the RBS [EBS] boron injection ensures that the core remains subcritical.

13.4.5.9.5.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

a) The amount of fuel rods experiencing DNB must remain less than 10 %.

b) The fuel pellet melting at the hot spot must not exceed 10 % by volume.

c) The peaking cladding temperature must remain less than 1482 °C.

For this accident, if the minimum DNBR remains above the design limit 1.30 (FC2000 correlation, deterministic method) [18], the criteria are met. Besides, the peak pressure of primary loop should remain below 22.37 MPa abs. to ensure the intactness of the primary side.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.9.5.3 Main Safety Functions

The safety functions used to cope with this accident are introduced as follows.

a) RT

The “Power range high neutron flux” signal triggers the reactor trip (FC1).

b) “ATWS” signal

The high rod position combined with RT signal triggers of the “ATWS” signal (FC2).

c) Turbine trip

The RT signal triggers the turbine trip (FC1).

d) The third group valves of the GCT [TBS] close

The RT signal triggers the third group valves of the GCT [TBS] close (FC3).

e) The forth group valves of the GCT [TBS] close

The RT signal delay 50 s triggers the forth group valves of the GCT [TBS] close (FC3).

f) RCP [RCS] pumps stop

The “SG level (narrow range) low 1” signal combined with the “ATWS” signal triggers the pumps to stop (FC2).

g) ARE [MFFCS] operation

The RT signal triggers the ARE [MFFCS] full load lines of the Steam Generator (SG) isolation automatically. The SGs are fed with water by the ARE [MFFCS] system through the low load lines (FC1).

h) ASG [EFWS] operation

The ASG [EFWS] is activated by the “SG level (wide range) low 2” signal (FC1).

i) PSVs open and closure

The PSVs open and close automatically to limit the primary pressure when the pressure reaches the set-point. The PSVs operation is a key mitigation measure for this accident, because it can maintain the primary pressure within the acceptance criterion (FC1).

j) VDA [ASDS] open and close

The VDA [ASDS] open and close automatically to limit the secondary pressure when the pressure reaches the set-point (FC1).

k) MSIV closure

The automatic MSIVs isolation is triggered by the “Pressure drop of SG high 1” signal or the “SG pressure low 1” signal (FC1).

l) RBS [EBS] operation

The “ATWS” signal initiates the RBS [EBS] operation automatically. The RBS [EBS], part of the DEC-A features, is one of the key systems to mitigate this accident (FC2).

13.4.5.9.5.4 Typical Events Sequences

An excessive increase in secondary system steam flow induces an overcooling of the primary side. This overcooling leads to a core power increase, by moderator reactivity

feedback effect, or by the action of the RCP [RCS] average temperature control. In this event, the reactor can be protected by “Overpower ΔT”, “Overtemperature ΔT” or “Power range high neutron flux” protection signal.

However, although the RT signal has been emitted, the control rods are still at high positions due to mechanical blockage. Therefore, the reactor trip is not realized. Then the turbine trips automatically. After that, the ARE [MFFCS] full load lines are automatically closed and the low load lines are unavailable. The RT signal also triggers the third group valves of the GCT [TBS] to close automatically and after 50 s the fourth group valves to close automatically.

The high rod position combined with RT signal leads to the triggering of the “ATWS” signal which initiates the RBS [EBS] operation.

The opening of the PSVs limits the primary pressure rise. The GCT [TBS] and the VDA [ASDS] ensure the removal of the secondary heat. When the SG level decreases to the “SG level (narrow range) low 1”, combined with the “ATWS” signal, the reactor coolant pumps stop automatically. When SG level decreases to the “SG level (wide range) low 2”, the ASG [EFWS] is started up to supply water to the SG automatically. The “SG pressure low 1” signal triggers the MSIVs to close automatically.

In the long term, the residual heat is removed by the VDA [ASDS] of all steam generators and the feedwater is supplied by the ASG [EFWS]. The RBS [EBS] boron injection ensures that the core remains subcritical. The final state of DEC-A is reached after the RHR is connected.

13.4.5.9.5.5 Analysis Assumptions

The detailed assumptions are presented in Reference [24]. The main assumptions are as follows:

13.4.5.9.5.5.1 Initial Conditions

a) Initial reactor power is the nominal power plus the maximum uncertainty to maximise the primary heat.

b) The initial reactor coolant flowrate is set as the thermal design flow, considering that 10 % of the SGs tubes are plugged.

c) The primary temperature is the rated value plus the maximum uncertainty to maximise primary heat.

d) The primary pressure is the rated value minus the maximum uncertainty to delay the PSVs open signal and penalize the DNBR.

e) The initial PZR level is the rated value minus the maximum uncertainty to penalize the DNBR.

13.4.5.9.5.5.2 Core-related Assumptions

The neutronic data are considered as follow:

a) The moderator temperature coefficient, is set at its maximum value (in absolute value) at the end of the transient, which envelopes 100% of the whole nuclear plant life time.

b) The Doppler power coefficient, which tends to limit the nuclear power increase, is set at its minimum value (in absolute value).

c) The Doppler temperature coefficient, which induces a nuclear power increase when the coolant temperature decreases, is set at its maximum value (in absolute value).

13.4.5.9.5.6 Results and Conclusions

The detailed assumptions are presented in Reference [24].

The minimum DNBR in the excessive increase in secondary system steam flow - ATWS accident is 1.93 greater than the limit 1.30 (FC2000 correlation, deterministic method). In the meantime, the peak primary pressure is 17.7 MPa abs, which does not exceed the maximum allowable pressure of 22.37 MPa abs. Therefore, the integrity of the RCP [RCS] is not challenged during the process of this accident. It is concluded that the acceptance criteria are met.

In the long term, the residual heat is removed by the VDA [ASDS] of all steam generators, the feedwater is supplied by the ASG [EFWS] and the RBS [EBS] boron injection ensures that the core remains subcritical. The final state of DEC-A is reached after the RHR is connected. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.9.6 ATWS by Rods Failure - Steam Line Break in Downstream of MSIV (State A)

13.4.5.9.6.1 Description

The causes of the ATWS may be:

a) Common cause failure of the protection system, especially protection system failure caused by software common cause failure.

b) Shutdown rods fail to be inserted into the core due to mechanical blockage of rods.

The Steam Line Break (SLB) - ATWS transient caused by mechanical blockage of rods is analysed in this report. The break locates at the downstream of MSIV and the double-ended guillotine break size is taken into consideration.

SLB will lead to the increase of SG steam flowrate, which causes the decrease of the

RCP [RCS] coolant temperature and RCP [RCS] pressure. It is an overcooling event and the positive reactivity is induced because of the negative moderator temperature feedback. This positive reactivity results in the nuclear power and thermal power augmentation, which challenges the DNBR design limit.

13.4.5.9.6.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows [7]:

d) The amount of fuel rods experiencing DNB must remain less than 10 %.

e) The fuel pellet melting at the hot spot must not exceed 10 % by volume.

f) The peaking cladding temperature must remain less than 1482 °C.

If the minimum DNBR remains above the design limit 1.30 (FC2000 correlation, deterministic method) [18], the criteria are met. Besides, the peak pressure of primary loop should remain below 22.37 MPa abs. to ensure the intactness of the primary side.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.9.6.3 Main Safety Functions

The following paragraphs present the main safety functions applied in ATWS caused by mechanical blockage combined with SLB.

a) RT signal

The RT signal is triggered by “Pressure drop of SG high 0” (FC1).

b) ATWS signal

The high rod position combined with RT signal triggers the ATWS signal (FC2).

c) Turbine trip

The RT signal triggers the turbine trip (FC1).

d) Main feedwater full load line isolation

Main feedwater full load lines of all SGs are isolated on RT signal (FC1).

e) MSIV isolation

The isolation of MSIV is triggered by “Pressure drop of SG high 1” (FC1).

f) ASG [EFWS] operation

The “SG level (wide range) low 2” signal starts up the ASG [EFWS] (FC1).

g) PSVs open and closure

The PSVs open and close automatically when the pressure reaches the setpoints to limit the primary pressure (FC1).

h) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches the "SG pressure high 1" setpoint to limit the secondary pressure (FC1).

i) RBS [EBS] operation

The ATWS signal starts up the RBS [EBS] operation automatically. The automatic start-up of RBS [EBS] is one of key functions to mitigate the accident, which belongs to the DEC-A features (FC2).

13.4.5.9.6.4 Typical Events Sequences

SLB will lead to a sudden increase of SG flowrate, which causes a decrease in SG pressure and induce the overcooling effect. The overcooling effect results in the decrease in RCP [RCS] coolant temperature and pressure, thus the positive reactivity is induced because of the negative moderator temperature feedback and the nuclear power and thermal power augment.

The RT signal is triggered by the "Pressure drop of SG high 0" signal. However, although the RT signal has been emitted, the control rods are still at high positions due to mechanical blockage. Therefore, the reactor trip is not realized and the nuclear power still increases. In the short term, the Doppler power feedback limits the rise of nuclear power.

The ATWS signal is triggered by high rod position combined with RT signal. The ATWS signal starts up the RBS [EBS] automatically to ensure the sub-criticality in the long term.

For the secondary side, The RT signal triggers the isolation of main feedwater full load lines of all SGs and operation of low load line of main feedwater. The isolation of MSIV is triggered by the "Pressure drop of SG high 1" signal to limit the overcooling effect. After the isolation of MSIV, the break is isolated and the primary pressure and temperature increase because of the reduction of SG heat removal capacity.

The opening of the PSVs limits the primary pressure rise, and the VDA [ASDS] ensures the removal of the secondary heat and limits the secondary pressure. When the SG level decreases to the "low SG level (wide range) low 2", the ASG [EFWS] is started up to supply water to the SG. In the long term, the core heat is removed by the VDA [ASDS] and low load lines of main feedwater or the ASG [EFWS].

13.4.5.9.6.5 Analysis Assumptions

The detailed assumptions are presented in Reference [25]. The main assumptions are as follows:

13.4.5.9.6.5.1.1 Initial Conditions

a) Initial reactor power is maximised, which is considered to maximise primary heat.

b) The primary temperature is maximised to minimise the DNBR.

c) The primary pressure is minimised to minimise the DNBR.

d) The initial pressuriser level is minimised to minimise the DNBR.

13.4.5.9.6.5.1.2 Core-related Assumptions

a) The minimum moderator temperature coefficient is adopted, which envelopes 100% of the whole nuclear plant life time.

b) The Doppler temperature coefficient is adopted at the same condition of the moderator temperature coefficient.

c) The Doppler power coefficient is adopted at the same condition of the moderator temperature coefficient.

13.4.5.9.6.6 Results and Conclusions

The detailed assumptions are presented in Reference [25].

The analysis shows the peak primary pressure is 19.75 MPa abs., which does not exceed the 130% design pressure (22.37 MPa abs.). The DNBR reaches its minimum value 1.53 at 20.4 seconds, which is above the design limit 1.30 (FC2000 correlation, deterministic method). It is concluded that the acceptance criteria are met.

The inherent safety of nuclear plant ensures the acceptance criteria concerning DNBR are satisfied. The opening of the PSV limits the primary pressure to guarantee the intactness of primary side. In the long term, the injection of RBS [EBS] ensures the sub-criticality, and the core heat is removed by the VDA [ASDS] and low load lines of main feedwater. The cooldowm of the secondary side ensures the RIS [SIS] connection condition in RHR mode is met, the reactor heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.10 SB-LOCA with Total Loss of MHSI (State A)

13.4.5.10.1 Description

SB-LOCA with total loss of MHSI is classified as a DEC-A accident, which is initiated by a small break located at the cold leg. The break size is considered as

equivalent diameters of 2.5 cm and 5.0 cm. The MHSI is assumed to be unavailable.

When SB-LOCA occurs, the break leads to the decrease of coolant inventory which cannot be compensated by RCV [CVCS]. The primary pressure reduces, the RT signal and SI signal are triggered in order. However, the MHSI fails to perform injection. The main consequence of the accident is the potential core exposure and heat-up.

The manual cooldown of the primary system should be performed as a key mitigation measure. In order to reach the injection pressure of LHSI, three trains of VDA [ASDS] are manually opened by the operator to depressurise the primary system. When the primary pressure decreases to the LHSI injection pressure, the LHSI begins to compensate the coolant inventory. In the long term, the decay heat is removed through the RHR.

13.4.5.10.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.10.3 Main Safety Functions

The following safety functions and operator actions are claimed in the analysis of SB-LOCA with total loss of MHSI.

a) Automatic protections

1) RT

The RT is triggered by the “Pressuriser pressure low 2” signal (FC1).

2) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

3) Isolation of ARE [MFFCS] full load line

After RT, the full load isolation valves of the ARE [MFFCS] are closed (FC1).

4) SI signal

The SI signal is triggered by the “Pressuriser pressure low 3” signal (FC1).

5) MCD

The MCD is initiated by SI signal and cools down the primary system with a cooling rate of 250 °C/h (FC1).

6) RCP [RCS] pumps

The RCP [RCS] pump trip is triggered by co-existence of RCP [RCS] Pumps ΔP low 1 signal and SI signal in two loops (FC1).

7) VDA [ASDS]

Three trains of VDA [ASDS] automatically open when the SG pressure reaches “SG pressure high 1” (FC1).

8) ASG [EFWS]

The ASG [EFWS] are actuated on “SG level (WR) low 2” signal (FC1).

b) Operator actions

1) RCP [RCS] boration

Two trains of RBS [EBS] are actuated by the operator to borate the RCP [RCS] (FC2).

2) Manual cooldown of the primary system.

In order to reach the injection pressure of LHSI, three trains of VDA [ASDS] are manually opened to perform the cooldown of primary system. In the case of 2.5 cm break, the cooling rate is { }. In the case of 5.0 cm break, the loss of coolant inventory is faster. The DEC-A feature LCD is performed to rapidly depressurise the primary system for efficient LHSI injection (FC2).

In this accident, the manual cooldown operation is a key mitigation measure since it depressurises the primary system and allows the LHSI to perform injection.

3) Accumulators isolation

During the RCP [RCS] depressurisation, the accumulators are isolated when the reactor coolant system pressure decreases below 2.0 MPa abs (FC2).

4) RIS [SIS] in RHR mode

The RHR is connected to the RCP [RCS] to ensure continuous heat removal and core long-term cooling (FC2).

13.4.5.10.4 Typical Events Sequences

The accident is initiated by a small break located at the cold leg. The break size is considered as equivalent diameters of 2.5 cm and 5.0 cm. The loss of coolant inventory cannot be compensated by RCV [CVCS].

The discharged coolant through the break leads to a decrease of primary pressure. The RT is triggered by “Pressuriser pressure low 2” signal. Then the turbine trip occurs and the ARE [MFFCS] full load isolation valves are closed coincident with RT. In the analysis of this accident, it is conservatively assumed that the low load pipelines of the ARE [MFFCS] are unavailable, and the ASG [EFWS] is used to control the SG level. The SG pressure rapidly increases to “SG pressure high 1” threshold after the turbine trip, the VDA [ASDS] automatically opens to prevent overpressure of secondary system. The PZR heaters are automatically switched off by “Pressuriser level low 3” signal.

When the primary pressure decreases to “Pressuriser pressure low 3” threshold, the SI signal is triggered. The RCP [RCS] pumps shutdown is triggered by co-existence of RCP [RCS] Pumps ΔP low 1 signal and SI signal in two loops. The SI signal activates MHSI and LHSI. However, the MHSI fails to actuate as an initiating event. The pressure in the primary system is high at this moment to prevent the injection of LHSI.

The SI signal also triggers MCD. The MCD cools down and depressurises the primary system with a cooling rate of 250 °C/h. When the MCD ends, the primary pressure remains high and prevents the injection of the RIS [SIS] accumulator or LHSI.

Manual actions are performed to mitigate the accident by the operator. Two RBS [EBS] pumps are manually actuated to inject borated water into the RCP [RCS]. Three trains of VDA [ASDS] are manually opened to depressurise the primary system. The RIS [SIS] accumulator or LHSI starts to inject water into the RCP [RCS] as soon as the injection pressure is reached. The water inventory is compensated and the RPV water level recovers. When the RIS [SIS] connection condition in RHR mode is met, the final state is reached.

13.4.5.10.5 Analysis Assumptions

The detailed assumptions are presented in Reference [26]. The main assumptions are as follows:

a) The accident is assumed to occur at full power state.

b) Initial reactor power is 102% FP, which is considered to maximise primary heat.

c) The reactor loop flowrate is the thermal design flowrate, which is considered to

penalise heat removal.

d) The RPV coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial pressuriser pressure is the nominal value plus the maximum uncertainty, which is considered to delay RT and SI signal.

f) The initial pressuriser level is the nominal level at power minus 7% based on uncertainties, which is considered to penalise water inventory.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise water inventory of secondary system.

h) The core bypass flowrate is maximum, which is considered to penalise heat removal.

i) After the RT, a conservative curve (2σ uncertainties on the "B+C term") is used for the core decay heat.

13.4.5.10.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [26]. In the case of 2.5 cm equivalent diameter break, the core remains covered during the whole transient. In the case of 5.0 cm equivalent diameter break, the peak cladding temperature is 357°C, which is much lower than the requirements (1204°C) in acceptance criteria. The maximum cladding oxidation is 0.004% of the cladding thickness, which is much lower than the requirements (17%) in acceptance criteria. The hydrogen generation is 0.003% of the amount that would have been generated if the whole active part of the cladding had reacted, which is far less than the requirements (1%) in acceptance criteria. The acceptance criteria are met. When the RIS [SIS] connection condition in RHR mode is met, the decay heat removal is ensured by the RHR in the long term. The final state of DEC-A is reached. The safe state is also reached once the RIS [SIS] is in operation in RHR mode.

13.4.5.11 TLOCC with Reactor Coolant Pump Sealing Leakage (State A)

13.4.5.11.1 Description

TLOCC with reactor coolant pump sealing leakage in state A refers to the total loss of RRI [CCWS] and SEC [ESWS] with leakage from the reactor coolant pump seals. It is a loss of coolant event, which might lead to decrease of pressuriser level and primary depressurisation with a possible core heat-up due to the lack of cooling. This accident belongs to DEC-A events.

In this accident analysis, the manual cooldown of the primary system should be performed as a key mitigation measure. In order to reach the injection pressure of

LHSI, three trains of VDA [ASDS] are manually opened by the operator to depressurise the primary system. When the primary pressure decreases to the LHSI injection pressure, LHSI begins to compensate the primary coolant inventory.

In the long term, the decay heat is removed through EHR [CHRS] and ECS [ECS].

13.4.5.11.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

However, if the core remains covered and the long term core cooling can be ensured during the transient, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.11.3 Main Safety Functions

The following safety functions are claimed in the analysis of TLOCC with reactor coolant pump sealing leakage.

a) Automatic functions

1) Reactor coolant pump

The reactor coolant pumps are stopped due to loss of seals injection and loss of the thermal barriers (FC2).

2) RT

The RT is triggered by the “Low RCP [RCS] pump speed” signal (FC1).

3) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

4) ARE [MFFCS]

ARE [MFFCS] full load lines of all SGs are isolated on RT signal (FC1).

5) VDA [ASDS]

Three trains of VDA [ASDS] open automatically when the SG pressure reaches “SG pressure high 1” to limit the secondary pressure (FC1).

6) SI signal

The SI signal is triggered by the “Pressuriser pressure low 3” signal (FC1).

7) MCD

The MCD is initiated by SI signal and cools down the primary system with a cooling rate of 250 °C/h (FC1).

8) ASG [EFWS]

Three trains of ASG [EFWS] are actuated by “SG level (wide range) low 2” signal, and the isolation of ASG [EFWS] is actuated by “SG level (wide range) high 1” signal (FC1).

9) DEL [SCWS]

The cooling of the LHSI pumps (train A and B) is automatically switched to the DEL [SCWS] by “RRI [CCWS] temperature high” or “RRI [CCWS] flowrate low” concomitant with “signal that train A or B LHSI pump is operating” to ensure the LHSI pumps (train A and B) in normal operation (FC3).

This safety function is a DEC-A feature, providing diverse cooling chains for LHSI pumps (train A and B) in normal operation. It is a key mitigation measure for this accident since it ensures the LHSI to perform injection.

b) Operator actions

1) Reactor coolant system boration

Two trains of RBS [EBS] are actuated by the operator to ensure the reactor is in the sub-critical state during the cooling stage (FC2).

2) Manual cooldown of the primary system

The cooldown is performed from MCR via the available VDA [ASDS] { } (FC2).

The controlled cooling operation is a key mitigation measure for this accident since it depressurises the primary system and allows the LHSI to perform injection.

3) Accumulators isolation

When the primary pressure reaches the isolation threshold, the accumulators are manually isolated by the operator (FC2).

13.4.5.11.4 Typical Events Sequences

TLOCC is induced by the unavailability of RRI [CCWS] and SEC [ESWS]. As a consequence of TLOCC, the following systems are assumed to be unavailable:

a) RCV [CVCS], including reactor coolant pump sealing injection.

b) All trains of the MHSI.

c) Train C of the LHSI.

d) Reactor coolant pumps thermal barriers.

e) The heat removal of secondary side is not affected by the TLOCC, and so the ASG [EFWS] and VDA [ASDS] remain available.

After the TLOCC with reactor coolant pump sealing leakage accident, it results in the loss of sealing injection and loss of the thermal barriers, consequently lead to the trip of the reactor coolant pumps. The “Low RCP [RCS] pump speed” signal triggers the RT. The RT signal leads to turbine trip and the isolation of the ARE [MFFCS] full load lines. After RT, SG water level is controlled by the low load pipelines of the ARE [MFFCS]. In the analysis of this accident, it is assumed that the low load pipelines of the ARE [MFFCS] are unavailable. And the ASG [EFWS] is used to control the SG level.

As the secondary side pressure increases, the VDA [ASDS] automatically opens to prevent secondary overpressure.

The SI signal is actuated on “Pressuriser pressure low 3” due to a break of the primary system, which starts the MHSI and LHSI system and initiates the MCD automatically, resulting in that the secondary side pressure reduces to 6.0 MPa abs. eventually. Due to the TLOCC, start-up of all MHSI and train C of the LHSI pump fails. The cooling of the other LHSI pumps (train A and B) is automatically switched to the DEL [SCWS], and then the LHSI pumps of trains A and B are available.

After the MCD operation, the primary pressure is still too high to allow injection by accumulators or LHSI (all MHSI are unavailable). Therefore, it is necessary for the operator to perform manual actions including actuation of the RBS [EBS] and manual cooldown of the primary system for the mitigation of the TLOCC accident. In order to decrease the primary pressure to the injection pressure of the accumulators and LHSI, the operator actuates two trains of the RBS [EBS] for reactor coolant system boration 30 minutes after the RT signal, and then performs the manual cooldown operation until the primary pressure is lower than the injection pressure of LHSI.

In the long term, the primary inventory is ensured by LHSI. The EHR [CHRS] is started manually to cool down the water of IRWST and containment according to the containment pressure criteria. The IRWST water temperature remains within the limit and the containment integrity is ensured. The final state is reached.

13.4.5.11.5 Analysis Assumptions

The detailed assumptions are presented in Reference [27]. The main assumptions are as follows:

a) The accident is assumed to occur at full power state, which is considered to maximise primary heat.

b) Initial reactor power is the nominal power plus the maximum uncertainty, which is considered to maximise primary heat.

c) The initial coolant flow rate is the thermal-hydraulic design flow rate, which is considered to penalise heat removal.

d) The RPV coolant average temperature is the rated value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial pressure of the pressuriser is the rated value plus the maximum uncertainty. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant.

f) The initial pressuriser level is the rated level at power minus 7% based on uncertainties. Because the less the initial primary inventory, the less core inventory after the break occurs.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise heat removal.

h) The total core bypass flowrate takes the maximum value (6.5%) to minimise the flow rate passing through the core, which is considered to penalise heat removal.

i) After the RT, a conservative curve (2σ uncertainties on the “B+C term”) is used for the core decay heat.

13.4.5.11.6 Result and Conclusion

The detailed results and conclusions for this accident (see Reference [27]) shows that the core remains covered during the whole process of the accident due to the lowest RPV water level (about 6.6 m) is higher than the top of the active core (5.724 m). In the long term, the part of residual heat is discharged into the containment through the reactor coolant pump seals break, and the other part is discharged out of the containment through the secondary side systems (ASG [EFWS] and VDA [ASDS]). Meanwhile, the spray mode of EHR [CHRS] is started manually to cool down the IRWST and containment as the ultimate heat sink. The heat need to be removed through EHR [CHRS] for this accident is bounded by SB-LOCA with total loss of LHSI due to the break size (the break size of the latter accident is about 20 cm^2, about double that of all RCP [RCS] seals leakage). As shown in SB-LOCA with total loss of LHSI, the IRWST temperature remains within the limit (120°C) to prevent the SI

pump cavitation and the containment pressure remains within the design pressure to ensure the containment integrity. As analysed above, the acceptance criteria are met for this accident.

13.4.5.12 TLOCC (States C3b and D)

13.4.5.12.1 Description

TLOCC in shutdown condition (states C3b and D) refers to the total loss of RRI [CCWS] and SEC [ESWS]. The TLOCC is classified as a DEC-A accident. Due to the initiating event, the following systems are unavailable:

a) RCV [CVCS]

b) All MHSI

c) Train C of LHSI

d) All RHR exchangers

In states C3b and D:

a) The RIS [SIS] is running in RHR mode.

b) The RCP [RCS] water level is greater than or equal to the lowest level of operation interval of RIS [SIS]/RHR, and less than the level when the reactor pool is filled.

c) The primary temperature is between 10 °C and 60 °C.

d) All RCP [RCS] pumps are stopped.

e) The RCP [RCS] is at the atmospheric pressure and in open state.

f) The SGs are unavailable to remove the decay heat.

The TLOCC accident in state C3b is considered as the bounding case for analysis because the decay heat of state C3b is greater than that of state D.

13.4.5.12.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core

geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

If the core remains covered and the long term core cooling can be ensured, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.12.3 Main Safety Functions

The following safety functions and operator actions are claimed in the analysis of TLOCC in state C3b.

a) Automatic protections

"RCP [RCS] loop level low 1" signal triggers the automatic LHSI actuation in SI reduced flowrate mode. This safety function is a DEC-A feature (FC3).

b) Operator actions

The EHR [CHRS] in spraying mode is manually actuated on the signal of high containment pressure or high water temperature of IRWST. This safety function is a DEC-A feature (FC3).

13.4.5.12.4 Typical Events Sequences

When the TLOCC occurs in state C3b, the RHR pump trip is automatically triggered and the residual heat removal becomes unavailable. The coolant temperature gradually increases to the saturation temperature. After the coolant becomes saturated, the decay heat is removed through the evaporation of the coolant, which leads to the decrease of the RCP [RCS] loop level. When "RCP [RCS] loop level low 1" threshold is reached, the actuation of LHSI in SI reduced flowrate mode is triggered. The LHSI which equips diversified cooling chain starts to compensate the coolant inventory.

The decay heat is transferred from the core to the containment through the evaporation continuously. The EHR [CHRS] in spraying mode is manually actuated to control the containment pressure and temperature. The EHR [CHRS] which equips diversified cooling supply removes the heat to the UHS through the ECS [ECS]. In the long term, the coolant inventory is maintained by the LHSI. The decay heat removal is ensured by the EHR [CHRS] and ECS [ECS].

13.4.5.12.5 Analysis Assumptions

The detailed assumptions are presented in Reference [13]. The main assumptions are as follows:

a) The TLOCC accident is assumed to occur in state C3b.

b) The RCP [RCS] water level is equal to the lowest level of operation interval of RIS [SIS]/RHR, which is considered to penalise the water inventory.

c) The RPV coolant average temperature is 60 °C, which is considered to maximise the primary heat.

d) The state C3b is reached at least 50.5 hours after the reactor shutdown. It is conservatively assumed that the decay heat is 15.48 MW.

13.4.5.12.6 Result and Conclusion

The detailed results and conclusions for this accident are presented in Reference [13]. The evaporation rate is about 6.858 kg/s. The actuation of LHSI in SI reduced flowrate mode is triggered by "RCP [RCS] loop level low 1". The total injection flowrate is 15 kg/s, which sufficiently compensates the evaporation of the coolant. The core remains covered during the whole transient. The acceptance criteria are met. After the actuation of two trains of EHR [CHRS], the water temperature in the IRWST is well limited, thus the LHSI pump cavitation is prevented. The containment pressure is maintained below the containment design pressure. In the long term, the decay heat is removed via the EHR [CHRS] and ECS [ECS]. The final state of DEC-A is reached.

13.4.5.13 Loss of Three PTR [FPCTS] Trains

13.4.5.13.1 Description

The loss of three PTR [FPCTS] trains accident refers to the failure of three PTR [FPCTS] trains, which leads to the total loss of SFP cooling. As the SFP cooling is failed, it leads to the increase of SFP water temperature. When the SFP water temperature reaches the saturation temperature, the decay heat of SFP is removed via the continuous evaporation of the SFP water.

As a main consequence, the SFP water is in a boiling state and is consumed continuously. Without any other protection functions, the spent fuel assemblies will be uncovered. And overpressure may occur in the fuel building.

In order to cope with this accident, the operator opens the water makeup line between the ASP [SPHRS] tank and SFP to feed the SFP. The damper and the rupture disc are designed to depressurise the fuel building.

13.4.5.13.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows:

a) The sub-criticality of the fuel assemblies is ensured.

b) The fuel assemblies in the fuel pool remain covered.

c) The decay heat from the spent fuel pool is removed.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.13.3 Main Safety Functions

The safety functions used to cope with this accident are introduced as follows.

a) SFP water makeup

The operator opens the water makeup line between the ASP [SPHRS] tank and SFP to feed the SFP (FC3).

b) Fuel building depressurisation

The operator opens the damper to depressurise the fuel building. If the damper is failed to open, the rupture disc is opened passively to avoid the over-pressure of fuel building (FC3).

13.4.5.13.4 Typical Events Sequences

The loss of three PTR [FPCTS] trains accident is considered as the DEC-A accident. When the three PTR [FPCTS] trains are failed, the cooling for SFP is lost. The SFP water temperature begins to increase. Then, the saturation temperature is reached and the SFP begins to boil. The SFP water begins to evaporate continuously and the SFP water level decreases. At the same time, the fuel building pressure increases.

As it takes several hours for the SFP water to increase to the saturation temperature, the function of SFP water makeup has already been ready before the SFP is boiling. When the SFP water level decreases, the operator opens the water makeup line between ASP [SPHRS] tank and SFP to feed the SFP. Thus the SFP water level is controlled in the normal operating value. The decay heat of SFP is removed by the water makeup and evaporation mode in the long term. In order to avoid the over-pressure of fuel building, the damper and rupture disc in the fuel building are used to control the fuel building pressure.

13.4.5.13.5 Analysis Assumptions

The detailed assumptions are presented in Reference [28]. The main assumptions are as follows:

a) The loss of three PTR [FPCTS] trains accident is assumed to happen in abnormal condition.

b) The initial decay heat in abnormal condition is the maximum.

c) The SFP water temperature is 50 °C which is the maximum normal operation temperature in abnormal condition.

d) The SFP water level is 16.9 m which is the minimum water level at normal operation.

e) The fuel building pressure is equal to the atmospheric pressure.

f) The atmospheric temperature of fuel building is 45 °C which is the maximum temperature at normal operation.

13.4.5.13.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [28]. It will take about 4.77 hours for the SFP water temperature to increase from 50 °C to 100 °C. The water evaporation rate is calculated to be 6.77 kg/s. The flow rate of water makeup from ASP [SPHRS] is about 13.8 kg/s, which is greater than the SFP water evaporation rate. So the fuel assemblies are covered during the whole accident process. The total water consumption is about 1755 m^3 for three days. The water inventory of ASP [SPHRS] tank is about 3035 m^3, which is greater than the total SFP water consumption. The sub-criticality of the fuel assemblies is ensured by the design of spent fuel storage rack.

It is concluded that the acceptance criteria mentioned above are met during the whole accident process. And the safe state is reached.

13.4.5.14 LUHS for 100 Hours (States A and B)

13.4.5.14.1 Description

LUHS for 100 hours (states A and B) refers to the total loss of the SEC [ESWS] and Circulating Water System (CRF [CWS]) or a complete failure of the pumping station in states A and B without leakage from the reactor coolant pump seals, and it belongs to DEC-A sequences. It is an overheating event, which might cause Reactor Coolant Pressure Boundary (RCPB) overpressure or fuel and cladding damage if no other mitigation measures applied. It might also induce the failure of the reactor coolant pump seals resulting in a primary system breakage, which is presented in reference [27].

In this report the present LUHS analysis is focused on the reactor coolant pump seals tightness and the secondary side feedwater consumption. For reactor coolant pump seals tightness, it is required that the temperature and pressure conditions of the final state can meet the safety requirements of the shaft seal system. For the secondary side feedwater consumption, as long as the SGs water supply is guaranteed, the residual heat from the core can be continuously removed. Therefore, the main mitigation measure for this event is the primary pressure and temperature control, and the refilling of the ASG [EFWS] tanks.

For LUHS in state B, the reactor has already tripped before the initiating event. Therefore, the reactor power is already reduced at the beginning of the transient. The

decay heat has to be removed through the SGs and the amount of decay heat needed to be removed is less than that in state A. In addition, the consumption of feedwater is much lower and the operator has more time to perform the refilling of the ASG [EFWS] tanks. Thus, the case in state B can be bounded by that of state A.

13.4.5.14.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. The accident should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204°C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would generate if the whole active part of the cladding had reacted.

d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

However, if the core remains covered and the long term core cooling can be ensured during the transient, above criteria are considered to be met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.14.3 Main Safety Functions

The following safety functions are claimed in the analysis of LUHS (100 hours).

a) Automatic functions

1) Reactor coolant pump

The reactor coolant pumps are stopped due to loss of seals injection and loss of the thermal barriers (FC2).

2) RT

The RT is triggered by the “Low RCP [RCS] pump speed” signal (FC1).

3) Turbine trip

The turbine trip is triggered by the RT signal (FC1).

4) ARE [MFFCS]

ARE [MFFCS] full load lines of all SGs are isolated on RT signal (FC1).

5) VDA [ASDS]

Three trains of VDA [ASDS] open automatically when the SG pressure reaches “SG pressure high 1” to limit the secondary pressure (FC1).

6) PSV

The PSVs automatically open when the opening set-point is reached (FC1).

7) ASG [EFWS]

Three trains of ASG [EFWS] are actuated by “SG level (wide range) low 2” signal, and the isolation of ASG [EFWS] is actuated by “SG level (wide range) high 1” signal (FC1).

b) Operator actions

1) Controlled cooling operation

The cooldown is performed from MCR via the available VDA [ASDS] by lowering their setpoints to { } (FC2).

The controlled cooling operation is a key mitigation measure for this accident. It can prevent the loss of integrity of the primary system due to the failure of the reactor coolant pump seals.

2) ASG [EFWS] tanks refilling

When all ASG [EFWS] tanks water level reaches the low 3 level, the operator opens the ASP [SPHRS] isolation valve manually on site to supply water makeup for the ASG [EFWS] storage tanks (FC3).

As mentioned above, LUHS (100 hours) analysis is focused on the secondary side feedwater consumption. So the refilling of the ASG [EFWS] tanks is a key safety function for this event.

13.4.5.14.4 Typical Events Sequences

LUHS is induced by the unavailability of SEC [ESWS] and CRF [CWS]. As a result, the following systems are assumed to be unavailable:

a) RRI [CCWS].

b) GCT [TBS].

c) RCV [CVCS], including reactor coolant pump seals injection.

d) All trains of the MHSI.

e) Train C of the LHSI.

f) Reactor coolant pump thermal barriers.

g) The heat removal of secondary side is not affected by the LUHS. As a result, the ASG [EFWS] and VDA [ASDS] remain available.

After the LUHS accident, the LUHS results in the loss of seals injection and loss of the thermal barriers, consequently leading to the trip of the reactor coolant pumps, while the shaft seal system can ensure the primary system integrity. The "Low RCP [RCS] pump speed" signal triggers the RT. The RT signal leads to turbine trip and the isolation of the ARE [MFFCS] full load lines. After RT, SG water level is controlled by the low load pipelines of the ARE [MFFCS]. In the analysis of this accident, it is assumed that the low load pipelines of the ARE [MFFCS] are unavailable, and the ASG [EFWS] is used to control the SG level.

Thirty minutes after the RT signal, the controlled cooling operation is performed manually by operator. The residual decay heat from core is removed by natural convection in the primary side, and transferred to the SGs. Meanwhile, steam is discharged from the secondary side into atmosphere through VDA [ASDS]. Finally, the pressure and temperature of the primary system can reach appropriate steady state to ensure the integrity of the reactor pump seals.

The SG feedwater is supplied by the ASG [EFWS]. Three ASG [EFWS] tanks can provide autonomy up to at least 24 hours of water supply for the SGs in state A. When the ASG [EFWS] tanks are drained, they can be refilled from the ASP [SPHRS] tank.

With above mitigation measures, the final state can be reached. It corresponds to that the core remains sub-critical and the long term core cooling can be ensured.

13.4.5.14.5 Analysis Assumptions

The detailed assumptions are presented in Reference [29]. The main assumptions are as follows:

a) The accident is assumed to occur at full power state, which is considered to maximise primary heat.

b) Initial reactor power is the nominal power plus the maximum uncertainty, which is considered to maximise primary heat, leading to more ASG [EFWS] water consumption.

c) The reactor loop flowrate is the thermal design flowrate, which is considered to penalise heat removal.

d) The RPV coolant average temperature is the nominal value plus the maximum uncertainty, which is considered to maximise primary heat.

e) The initial pressuriser pressure is the nominal value plus the maximum uncertainty, which is considered to penalise the conditions of RCP [RCS] seals tightness.

f) The initial pressuriser level is the nominal level at power plus 7% based on uncertainties, which is considered to penalise the conditions of RCP [RCS] seals tightness and primary heat.

g) The initial SG level is the nominal level at power minus 10% based on uncertainties, which is considered to penalise water inventory of SGs and the heat removal by secondary side.

h) The core bypass flowrate is maximum, which is considered to penalise heat removal.

i) After the RT, a conservative heat curve (1.645σ uncertainties on the "B+C term") is used for the core decay heat.

13.4.5.14.6 Result and Conclusion

The detailed results and conclusions for this accident (see Reference [29]) shows that the core remains covered during the whole process of the accident due to the lowest RPV water level (11.16 m) is higher than the top of the active core (5.724 m). In the long term, the pressure and temperature of the primary system comply with the requirements of reactor pump seals tightness to ensure the primary inventory. As regard to ASG [EFWS] water consumption, a total of 3291t of feedwater is estimated to be necessary for LUHS during 100 hours. Compared to the available feedwater (at least a total of 4745t), there are enough margins for ASG [EFWS] tanks refilling. Therefore, the capacity of residual heat removal by secondary side is always sufficient.

As analysed above, the acceptance criteria are met for this accident.

13.4.5.15 Uncontrolled Primary Water Level Drop without SI Signal from RPS [PS] (States C3b and D)

13.4.5.15.1 Description

The uncontrolled primary water level drop without SI signal from RPS [PS] (State C3b and D) accident is initialised by the decrease of RCP [RCS] water level due to the failure of water level control. When the RCP [RCS] water level decreases to the "RCP [RCS] loop level low 1" threshold, the SI signal is not emitted because of the failure of RPS [PS].

As the main consequence, the accident will lead to the cavitation of RIS [SIS]/ RHR pumps. And the core may be uncovered.

In order to cope with this accident, a diversified SI signal is designed to trigger the RIS [SIS] actuation.

13.4.5.15.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. The

detailed acceptance criteria used for this accident are as follows:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted.

d) The core geometry shall remain coolable, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptable low value and the decay heat shall be removed.

If the core keeps covered during the whole accident course, the acceptance criteria mentioned above can be met. Besides, the RIS [SIS]/RHR pumps shall be prevented from any cavitation risk, which means the RCP [RCS] water level shall be higher than the cavitation water level of RIS [SIS]/RHR during the whole accident course.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.15.3 Main Safety Functions

The safety functions used to cope with this accident are introduced as follows.

a) RIS [SIS]

The RIS [SIS] is actuated by the diversified “RCP [RCS] loop level low 1” signal (FC2).

b) RCV [CVCS]

After the diversified SI signal, the RCV [CVCS] letdown line is isolated (FC2).

13.4.5.15.4 Typical Events Sequences

The uncontrolled primary water level drop without SI signal from RPS [PS] happens in C3b or D state. As the control of RCP [RCS] water level is failed, the RCP [RCS] water level begins to decrease. Later, the “RCP [RCS] loop level low 1” threshold is reached, but the SI signal from RPS [PS] is not emitted to actuate the RIS [SIS].

The RCP [RCS] water level continues to decrease until reaching the diversified “RCP [RCS] loop level low 1” threshold. Then, the MHSI is actuated on diversified “RCP [RCS] loop level low 1” signal to feed the RCP [RCS]. After the actuation of the MHSI, the RCP [RCS] water level begins to increase. At the same time, the RCV [CVCS] letdown line is isolated after the diversified SI signal.

In the long term, the core decay heat is removed by the RIS [SIS] in RHR mode.

13.4.5.15.5 Analysis Assumptions

The detailed assumptions are presented in Reference [30]. The main assumptions are as follows:

a) The RCP [RCS] coolant average temperature is assumed to be 60 °C, which minimises the primary coolant density. This assumption also minimises the water inventory between diversified "RCP [RCS] loop level low 1" threshold and RIS [SIS]/RHR pumps cavitation level.

b) The RCP [RCS] water level is assumed to be the middle-loop water level conservatively, which minimises the RCP [RCS] water inventory.

c) The RCP [RCS] pressure is equal to the atmospheric pressure.

d) The initial decay heat of state C3b is greater than that of state D. Thus, the decay heat of state C3b is used for the accident analysis. The state C3b is reached at least 50.5 hours after the reactor shutdown. The initial decay heat in this state is approximately 15.48 MW.

13.4.5.15.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [30]. The 75t/h is considered as the RCV [CVCS] letdown flow rate, so the time between reaching the "RCP [RCS] loop level low 1" threshold and RIS [SIS]/RHR pump cavitation level is 41.6 seconds. The MHSI can be actuated 28 seconds after reaching the diversified "RCP [RCS] loop level low 1" threshold.

Consequently, The RCP [RCS] water level drop stops before reaching the RIS [SIS]/RHR pump cavitation level. And the RIS [SIS] in RHR mode remains in normal operation during the whole accident course. The acceptance criteria mentioned are met during the whole accident, and the DEC-A final state is reached. The safe sate is also reached via the continuous heat removal of the RIS [SIS] in RHR mode.

13.4.5.16 Multiple SG Tubes Rupture (10 tubes) (State A)

13.4.5.16.1 Description

The multiple SGTR (10 tubes) (State A) leads to a decrease of primary pressure and loss of primary coolant. The radiological coolant enters into the Affected Steam Generator (SGa) and is released to the environment directly when the VDA [ASDS] opens automatically.

As the main consequence of this accident, the radioactivity of the primary system is transferred to the SGa due to the SGTR and is then discharged to the environment directly. And the risk of core uncovery also exists.

In order to cope with this accident, the RCP [RCS] cooldown { } is performed manually. And the APG [SGBS] transfer line is opened to control the SGa water level.

13.4.5.16.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted.

d) There shall be no overflow occurred in SGa.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.16.3 Main Safety Functions

The automatic and manual safety functions used to cope with this accident are introduced as follows.

a) Automatic functions

1) High activity in the Plant Radiation Monitoring System (KRT [PRMS]) signal

As the high activity in the Main Steam System (VVP [MSS]) is detected by KRT [PRMS], an alarm is actuated (FC1).

2) RT

RT is triggered on “Pressuriser pressure low 2” signal (FC1).

3) Turbine trip

The turbine trip is triggered after the RT (FC1).

4) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT (FC1).

5) RIS [SIS]

The RIS [SIS] is actuated on “Pressuriser pressure low 3” signal (FC1).

6) MCD

The MCD is initiated automatically with a cooling rate of 250 °C/h to cool down the

primary side after the SI signal (FC1).

7) RCV [CVCS]

The RCV [CVCS] charging line and the RCP [RCS] pumps seal injection are both isolated on “SG level (NR) high 2 after MCD finished” signal (FC1). The RCV [CVCS] letdown is isolated on “Pressuriser level low 1 and RT” signal (FC1).

8) MSIV

The MSIVs are closed on “SG level (NR) high 2 after MCD finished” signal (FC1).

9) VDA [ASDS]

The VDA [ASDS] opens automatically on “SG pressure high 1” signal (FC1). Based on the “SG level (NR) high 2 after MCD finished” signal, the VDA [ASDS] isolation is triggered. And the setpoint of VDA [ASDS] in affected loop increases to { } which is between the MHSI delivery pressure and MSSV opening setpoint (FC1).

10) ASG [EFWS]

The Emergency Feedwater Systems (ASGs [EFWSs]) are actuated on “SG level (WR) low 2” signal (FC1).

b) Operator Actions

1) SGa isolation

The operator performs or confirms the isolation of SGa, including the ARE [MFFCS] and ASG [EFWS] isolation, MSIV closure and increase of the VDA [ASDS] setpoint (FC2).

2) RCP [RCS] cooldown

The RCP [RCS] cooldown { } is performed manually via the VDA [ASDS] and ASG [EFWS] in unaffected loops (FC2).

3) RCP [RCS] boration

The RBS [EBS] trains are actuated by the operator in order to borate the RCP [RCS] (FC2).

4) Control of MHSI

Three trains of MHSI are controlled manually by the operator. They will be closed gradually during the accident in order to decrease the primary pressure (FC2).

5) Accumulator (ACC) isolation

Three Accumulators (ACCs) are isolated manually by the operator during the accident (FC2).

6) APG [SGBS] transfer line opening

The APG [SGBS] transfer line is opened by the operator to reduce the water inventory of the SGa (FC2).

7) RCP [RCS] depressurisation

The operator performs the final RCP [RCS] depressurisation via the VDA [ASDS] in the affected loop in order to reach the RHR connecting pressure (FC2).

8) RIS [SIS] in RHR mode connection

The RIS [SIS] in RHR mode is connected to the RCP [RCS] to remove the decay heat continuously (FC2).

13.4.5.16.4 Typical Events Sequences

The multiple SGTR (10 tubes) is considered as the DEC-A accident. When the double-ended rupture of 10 SG tubes happens, it is detected by the high activity in KRT [PRMS] signal. The PZR pressure decreases rapidly, and the RT is triggered on "Pressuriser pressure low 2" signal. After the RT signal, the full load lines of ARE [MFFCS] are isolated and the turbine trip is initiated automatically. The low load lines of ARE [MFFCS] are assumed to be isolated together with full load lines of ARE [MFFCS] during the accident analysis to maximises the steam release to the environment.

Because of the continuous coolant leakage from primary side to SGa, the PZR level decreases. The PZR heaters are closed when the "Pressuriser level low 3" signal occurs. And the RCV [CVCS] letdown line is isolated on "Pressuriser level low 1 and RT" signal.

As the PZR pressure decreases continuously, the RIS [SIS] is actuated on "Pressuriser pressure low 3" signal, and an automatic MCD with a cooling rate of 250 °C/h is initiated after the SI signal.

The SGa water level increases continuously and will reach the "SG level (NR) high 2" threshold. Based on the "SG level (NR) high 2 after MCD finished" signal, the RCV [CVCS] charging line and the RCP [RCS] pumps seal injection are both isolated. The MSIV in loop 1 closes automatically. And the setpoint of the VDA [ASDS] in loop 1 increases to { } which is between the MHSI delivery pressure and MSSV opening setpoint.

At about 1800.0 seconds, the operator performs manual actions to continue the accident mitigation. The operator confirms the isolation of SGa, although most actions of the SGa isolation are finished by automatic protection functions before. Then, the operator closes two MHSI trains but remains one MHSI train to feed the RCP [RCS].

After manual actuation of two RBS [EBS] trains, the operator performs the manual

cooldown { } via the unaffected SG to cool down the RCP [RCS]. As the performance of RCP [RCS] cooldown, the water inventory of unaffected SG is consumed continuously. The ASG [EFWS] in loop 2 and 3 are actuated on "SG level (WR) low 2" signal.

With setpoint increase of the VDA [ASDS] in loop 1 and performance of the manual RCP [RCS] cooldown, the steam release to the environment is almost terminated.

When the primary pressure decreases below { }, three ACCs are isolated in order to decrease the coolant leakage from primary to secondary side. When the core outlet temperature decreases below { }, the last MHSI train is closed.

As the water level of SGa is too high, the operator opens the APG [SGBS] transfer line to transfer the water from the SGa to the partner SG. And it is necessary to isolate the partner SG before the opening of the APG [SGBS] transfer line.

When the water level of SGa is lower than the "SG level (WR) high 1" threshold, the operator performs the final RCP [RCS] depressurisation via the VDA [ASDS] in loop 1 in order to reach the RHR connecting pressure. When the RHR connecting pressure is reached, the VDA [ASDS] in the loop 1 is closed manually again.

Finally, the RIS [SIS] in RHR mode is connected to the RCP [RCS] to remove the decay heat in the long term. And the DEC-A final state is reached.

13.4.5.16.5 Analysis Assumptions

The detailed assumptions are presented in Reference [31]. The main assumptions are as follows:

a) The multiple SGTR (10 tubes) is considered to happen at full power.

b) The rupture is located in the lower part of the SG tubes bundle on the cold side, which maximises the SGTR leak flowrate.

c) The initial state is at 102% nominal power, which maximises the primary heat.

d) The thermal design value is considered for the primary flowrate, which penalises heat removal of unaffected SGs.

e) After the RT, a conservative decay heat curve (1.645σ uncertainties on the "B+C term") is used to represent the residual power history.

13.4.5.16.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [31]. During the whole accident process, the peak cladding temperature is less than 360 °C which remains lower than 1204 °C. The maximum cladding oxidation is about 0.00315% of the cladding thickness which is lower than 17%. The maximum hydrogen generation is about 0.00193% which remains lower than 1% of the amount

that would be generated if the whole active part of the cladding had reacted. The largest volume liquid fraction of the SGa upper part is about 0.03%, which means that no overflow occurs in the SGa. Consequently, the acceptance criteria mentioned are met. The plant can be led to the final state with limiting the radioactivity release to the environment.

13.4.5.17 MSLB with SGTR (1 tube) in the Affected SG (State A)

13.4.5.17.1 Description

The MSLB leads to a fast depressurisation of the secondary side and a sudden increase of the heat removal from primary to secondary side, which is an overcooling accident for the core. After the SGTR occurs in the same loop as the MSLB, the primary coolant is transferred from primary side to the SGa and released to the environment via the MSLB and VDA [ASDS].

As the main consequence of this accident, the MSLB may lead to the reactor power rise because of the negative moderator temperature feedback. The sudden reactor power rise may lead to the damage of the fuel and cladding. Due to the SGTR, the radioactivity of the primary system is transferred to the SGa and is then discharged to the environment directly through the MSLB and the VDA [ASDS].

In order to cope with this accident, the RCP [RCS] cooldown {
} is performed manually. And the APG [SGBS] transfer line is opened to control the SGa water level.

13.4.5.17.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted.

d) There shall be no overflow occurred in SGa.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.17.3 Main Safety Functions

The automatic and manual safety functions used to cope with this accident are introduced as follows:

a) Automatic functions

1) High activity in the KRT [PRMS] signal

As the high activity in the VVP [MSS] is detected by KRT [PRMS], an alarm is actuated (FC1).

2) RT

RT is triggered on “Pressure drop of SG high 1” signal (FC1).

3) Turbine trip

The turbine trip is triggered after RT (FC1).

4) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT (FC1).

5) RCV [CVCS]

The RCV [CVCS] letdown is isolated on “Pressuriser level low 1 and RT” signal (FC1).

6) MSIV

The MSIV are closed on “Pressure drop of SG high 1” signal (FC1).

7) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1” threshold (FC1).

8) ASG [EFWS]

The ASGs [EFWSs] are actuated on “SG level (WR) low 2” signal (FC1).

b) Operator Actions

1) SGa isolation

The operator performs or confirms the isolation of SGa, including the ARE [MFFCS] and ASG [EFWS] isolation, MSIV closure and increase of the VDA [ASDS] setpoint (FC2).

2) RCV [CVCS] charging line isolation

The RCV [CVCS] charging line is isolated manually by the operator in order to decrease the coolant leakage from primary side to SGa (FC2).

3) RCP [RCS] cooldown

The RCP [RCS] cooldown { } is performed manually via the VDA [ASDS] and ASG [EFWS] in unaffected loops (FC2).

4) RCP [RCS] boration

The RBS [EBS] trains are actuated by the operator in order to borate the RCP [RCS] (FC2).

5) Control of MHSI

Three trains of MHSI are controlled manually by the operator. They will be closed gradually during the accident in order to decrease the primary pressure (FC2).

6) ACC isolation

Three ACCs are isolated manually by the operator during the accident (FC2).

7) APG [SGBS] transfer line opening

The APG [SGBS] transfer line is opened by the operator to reduce the water inventory of the SGa (FC2).

8) RCP [RCS] depressurisation

The operator performs the final RCP [RCS] depressurisation via the VDA [ASDS] in the affected loop in order to reach the RHR connecting pressure (FC2).

9) RIS [SIS] in RHR mode connection

The RIS [SIS] in RHR mode is connected to the RCP [RCS] to remove the decay heat continuously (FC2).

13.4.5.17.4 Typical Events Sequences

The MSLB and SGTR (1 tube) happen at the beginning of the accident. The MSLB with double-ended rupture of steam line happens in the loop 1 initially. And the SGTR with double-ended rupture of one SG tube happens in the same loop as the MSLB. The SGTR is located in the lower part of the SG tubes bundle on the cold side. This location maximises the SGTR leak flowrate.

Because of the MSLB, the pressure of secondary side decreases sharply. The RT is triggered on “Pressure drop of SG high 1” signal. And the MSIVs are closed on “Pressure drop of SG high 1” signal at the same time.

After the RT signal, the full load lines of ARE [MFFCS] are isolated and the turbine trip is initiated automatically. The low load lines of ARE [MFFCS] are assumed to be isolated together with full load lines of ARE [MFFCS] during the accident analysis to maximises the steam release to the environment.

After the turbine trip, the secondary pressure increases to the VDA [ASDS] opening setpoint and the VDA [ASDS] opens automatically.

When the double-ended rupture of one SG tube happens, it is detected by the high activity in KRT [PRMS] signal. The PZR level decreases continuously because of the continuous coolant leakage from primary side to SGa. The RCV [CVCS] letdown line

is isolated on “Pressuriser level low 1 and RT” signal. And the PZR heaters are turned off when the “Pressuriser level low 3” signal occurs.

At about 1800.0 seconds, the operator performs manual actions to continue the accident mitigation. The operator confirms the isolation of SGa. Some actions of the SGa isolation are finished by automatic protection functions before. The ASG [EFWS] of loop 1 is isolated manually by the operator although it does not actuate automatically before. And the setpoint of the VDA [ASDS] in loop 1 is set to { } by the operator.

In order to feed the RCP [RCS], the operator keeps one MHSI train in service. Then, the operator isolates the RCV [CVCS] charging line in order to decrease the coolant leakage from primary side to SGa.

After manual actuation of two RBS [EBS] trains, the operator performs the RCP [RCS] cooldown { } via the unaffected SGs. As performance of the manual RCP [RCS] cooldown, the water level of unaffected SGs decreases continuously. The ASG [EFWS] trains in loop 2 and 3 are actuated on “SG level (WR) low 2” signal.

When the primary pressure decreases below { }, three ACCs are isolated in order to decrease the coolant leakage from primary to secondary side. When the core outlet temperature decreases below { }, the last MHSI train is closed.

As the water level of SGa is too high, the operator opens the APG [SGBS] transfer line to transfer the water from the SGa to the SG in loop 2. And it is necessary to isolate the SG in loop 2 before the opening of the APG [SGBS] transfer line.

After opening of the APG [SGBS] transfer line, the water level of SGa decreases continuously. When the water level of SGa is lower than the “SG level (WR) high 1” threshold, the operator performs the final RCP [RCS] depressurisation via the VDA [ASDS] in loop 1 in order to reach the RHR connecting pressure. When the RHR connecting pressure reaches, the VDA [ASDS] in the loop 1 is closed manually again.

Finally, the RIS [SIS] in RHR mode is connected to the RCP [RCS] to remove the decay heat in the long term.

13.4.5.17.5 Analysis Assumptions

The detailed assumptions are presented in Reference [32]. The main assumptions are as follows:

a) The MSLB and SGTR (1 tube) is considered to happen at full power.

b) The rupture is located in the lower part of the SG tubes bundle on the cold side, which maximises the SGTR leak flowrate.

c) The initial state is at 102% nominal power, which maximises the primary heat.

d) The thermal design value is considered for the primary flowrate, which penalises heat removal of unaffected SGs.

e) After the RT, a conservative decay heat curve (1.645σ uncertainties on the "B+C term") is used to represent the residual power history.

13.4.5.17.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [32]. During the whole accident process, the peak cladding temperature is less than 360 °C which remains lower than 1204 °C. The maximum cladding oxidation is about 0.000527% of the cladding thickness which is lower than 17%. The maximum hydrogen generation is about 0.00278% which remains lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted. The largest volume liquid fraction of the SGa upper part is about 0.105%, which means that no overflow occurs in the SGa. Consequently, the acceptance criteria mentioned are met. The plant can be led to the final state with limiting the radioactivity release to the environment.

13.4.5.18 SGTR (1 tube) with VDA [ASDS] Stuck Open in the Affected SG (State A)

13.4.5.18.1 Description

The SGTR (1 tube) with VDA [ASDS] stuck open in the SG affected (State A) is initiated by a double-ended rupture of one SG tube. The VDA [ASDS] in the same loop as the SGa remains stuck open since it has opened, which forms a non-isolable flow path between the primary system and the environment.

As the main consequence of this accident, the radioactivity of the primary system is transferred to the SGa due to the SGTR and is then discharged to the environment directly through the stuck open VDA [ASDS].

In order to cope with this accident, the LCD is performed to decrease the primary pressure and temperature rapidly. Then, the RIS [SIS] in RHR mode is connected to the primary side to continue the decrease of primary pressure and temperature. The detailed accident analysis is described in the following chapters.

13.4.5.18.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted.

d) There shall be no overflow occurred in SGa.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.18.3 Main Safety Functions

The automatic and manual safety functions used to cope with this accident are introduced as follows.

a) Automatic functions

1) High activity in the KRT [PRMS] signal

As the high activity in the VVP [MSS] is detected by KRT [PRMS], an alarm is actuated (FC1).

2) RT

RT is triggered on “Pressuriser pressure low 2” signal (FC1).

3) Turbine trip

The turbine trip is triggered after RT (FC1).

4) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT (FC1).

5) RIS [SIS]

The RIS [SIS] is actuated on “Pressuriser pressure low 3” signal (FC1).

6) MCD

The MCD is initiated automatically with a cooling rate of 250 °C/h to cool down the primary side after the SI signal (FC1).

7) RCP [RCS] pumps

The “RCP [RCS] pump △P low 1 and SI” signal triggers the RCP [RCS] pumps trip (FC1).

8) RCV [CVCS]

The RCV [CVCS] charging line is isolated on “SG pressure low 4 and SI” signal (FC1). The RCV [CVCS] letdown is isolated on “Pressuriser level low 1 and RT” signal (FC1).

9) MSIV

The MSIV are closed on “Pressure drop of SG high 1” signal (FC1).

10) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1” threshold (FC1).

11) ASG [EFWS]

The ASGs [EFWSs] are actuated on “SG level (WR) low 2” signal (FC1).

b) Operator Actions

1) SGa isolation

The operator performs or confirms the isolation of SGa, including the ARE [MFFCS] and ASG [EFWS] isolation, MSIV closure and increase of the VDA [ASDS] setpoint (FC2).

2) LCD

The LCD is performed through the unaffected SG to cool down the RCP [RCS] rapidly. This action consists of the opening of all VDA [ASDS] trains and a stepwise pressure reduction leading to full opening of all VDA [ASDS] control valves (FC2).

3) RCP [RCS] boration

The RBS [EBS] trains are actuated by the operator in order to borate the RCP [RCS] (FC2).

4) Control of MHSI

Three trains of MHSI are controlled manually by the operator. They will be closed gradually during the accident in order to decrease the primary pressure (FC2).

5) ACC isolation

Three ACCs are isolated manually by the operator during the accident (FC2).

6) RIS [SIS] in RHR mode connection

The RHR is connected to the RCP [RCS] to remove the decay heat continuously (FC2).

13.4.5.18.4 Typical Events Sequences

The SGTR (1 tube) with VDA [ASDS] stuck open in the affected SG is considered as the DEC-A accident.

When the double-ended rupture of one SG tube happens, it is detected by the high activity in KRT [PRMS] signal. The PZR level decreases continuously because the SGTR leakage cannot be compensated by the RCV [CVCS]. The PZR heaters are turned off when the “Pressuriser level low 3” signal occurs.

The primary pressure also decreases, and the RT is triggered on “Pressuriser pressure low 2” signal. After the RT signal, the full load lines of ARE [MFFCS] are isolated

and the turbine trip is initiated automatically. The low load lines of ARE [MFFCS] are assumed to be isolated together with full load lines of ARE [MFFCS] during the accident analysis to maximises the steam release to the environment. And the RCV [CVCS] letdown line is isolated on “Pressuriser level low 1 and RT” signal.

After the turbine trip, the SGa pressure increases rapidly and reaches the “SG pressure high 1” threshold. The VDA [ASDS] of loop 1 opens automatically and remains stuck open, which leads to a fast decrease of secondary side pressure. The MSIV closes on “Pressure drop of SG high 1” signal.

As the PZR pressure decreases continuously, the RIS [SIS] is actuated on “Pressuriser pressure low 3” signal, and an automatic MCD with a cooling rate of 250 °C/h is initiated after the SI signal. When the SGa pressure decreases to the “SG pressure low 4” threshold, the RCV [CVCS] charging line is isolated on “SG pressure low 4 and SI” signal.

As the stuck open of VDA [ASDS] in loop 1, the SGa water inventory loses rapidly. The ASG [EFWS] in loop 1 is actuated on “SG level (WR) low 2” signal.

At about 1800.0 seconds, the operator performs manual actions to continue the accident mitigation. The operator confirms the isolation of SGa, although most actions of the SGa isolation are finished by automatic protection functions before. The ASG [EFWS] of loop 1 is closed manually by the operator. Then, the operator closes two MHSI trains but remains one MHSI train to feed the RCP [RCS].

After manual actuation of two RBS [EBS] trains, the operator performs the LCD via the unaffected SG to cool down the RCP [RCS]. As the performance of LCD, the water level of unaffected SG decreases rapidly. The ASG [EFWS] in loop 2 and 3 are actuated on “SG level (WR) low 2” signal.

When the primary pressure decreases below { }, three ACCs are isolated in order to decrease the coolant leakage from primary to secondary side. When the core outlet temperature decreases below { }, the last MHSI train is closed.

After the closure of the last MHSI, the primary pressure decreases and reaches the connecting pressure of RHR. The RHR is connected to the RCP [RCS] to remove the decay heat in the long term.

When the two RBS [EBS] trains are closed, the coolant leakage of SGTR is almost terminated. When the primary coolant temperature is below 100 °C, and the primary pressure is near to the atmospheric pressure. The steam release from the stuck open VDA [ASDS] is almost terminated.

13.4.5.18.5 Analysis Assumptions

The detailed assumptions are presented in Reference [33]. The main assumptions are as follows:

a) The SGTR (1 tube) with VDA [ASDS] stuck open in the affected SG is considered to happen at full power.

b) The rupture is located in the lower part of the SG tubes bundle on the cold side, which maximises the SGTR leak flowrate.

c) The initial state is at 102% nominal power, which maximises the primary heat.

d) The thermal design value is considered for the primary flowrate, which penalises heat removal of unaffected SGs.

e) After the RT, a conservative decay heat curve (1.645σ uncertainties on the "B+C term") is used to represent the residual power history.

13.4.5.18.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [33]. During the whole accident process, the peak cladding temperature is less than 360 °C which remains lower than 1204 °C. The maximum cladding oxidation is about 0.00055% of the cladding thickness which is lower than 17%. The maximum hydrogen generation is about 0.00194% which remains lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted. The largest volume liquid fraction of the SGa upper part is about 0.092%, which means that no overflow occurs in the SGa. Consequently, the acceptance criteria mentioned are met. The plant can be led to the final state with limiting the radioactivity release to the environment.

13.4.5.19 TLOCC with Loss of Secondary Cooldown (failure of ASG [EFWS] or VDA [ASDS]) (State A)

13.4.5.19.1 Description

The TLOCC with loss of secondary cooldown (State A) accident refers to the total loss of RRI [CCWS] and SEC [ESWS]. Meanwhile, the secondary cooldown is unavailable because of the failure of all ASG [EFWS] or VDA [ASDS]. Due to the TLOCC, the following systems or equipment are unavailable:

a) RCV [CVCS].

b) All trains of MHSI.

c) Train C of the LHSI.

d) RCP [RCS] pumps thermal barriers.

The TLOCC with loss of secondary cooldown is an overheating accident. Due to the loss of secondary cooldown, the primary pressure will increase to the opening setpoint of PSVs and the primary coolant is discharged continuously via PSVs. As the main consequence, the core may be uncovered.

In order to mitigate this accident, the ASP [SPHRS] is designed to remove the primary heat. The detailed accident analysis is described in the report.

13.4.5.19.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are adopted as targets. The detailed acceptance criteria used for this accident are as follows:

a) The peak cladding temperature must remain lower than 1204 °C.

b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness.

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted.

d) The core geometry shall remain coolable, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.

e) The long term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptable low value and the decay heat shall be removed.

If the core is not uncovered and the long term core cooling can be ensured, it can be deduced that the criteria above are met.

In terms of radiological consequence, it is evaluated in Sub-chapter 13.4.6 and Sub-chapter 13.4.7.

13.4.5.19.3 Main Safety Functions

The safety functions used to cope with this accident are introduced as follows.

a) RCP [RCS] pumps

The RCP [RCS] pumps are stopped due to the loss of sealing injection and thermal barriers (FC2).

b) RT

RT is triggered on “Low RCP [RCS] pump speed” signal (FC1).

c) Turbine trip

The turbine trip is triggered after the RT (FC1).

d) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT (FC1).

e) PSV

The PSVs automatically open when the opening setpoint is reached (FC1).

f) MSSV

The MSSVs automatically open when the opening setpoint is reached (FC1).

g) ASP [SPHRS]

Three trains of ASP [SPHRS] are actuated on “SG level (wide range) low 3 combined with ASG [EFWS] flow rate low continues 60 seconds” signal (FC3).

13.4.5.19.4 Typical Events Sequences

The TLOCC with loss of secondary cooldown is a DEC-A accident. The TLOCC results in the loss of seal injections and thermal barriers for RCP [RCS] pumps, leading to the trip of the RCP [RCS] pumps consequently. Then, the “Low RCP [RCS] pump speed” signal triggers the RT. The RT signal leads to turbine trip and the isolation of the ARE [MFFCS] full load lines. After the RT, SG water levels are controlled by the low load lines of ARE [MFFCS]. In the analysis of this accident, it is assumed that the low load lines of ARE [MFFCS] are unavailable.

After the turbine trip, the secondary pressure increases continuously. As all VDA [ASDS] are failed, the secondary pressure is reached to the opening setpoint of MSSVs and the MSSVs open automatically to avoid the secondary overpressure. The coolant in SGs is discharged continuously through opening of MSSVs. The coolant consumption of SGs cannot be compensated by the ASG [EFWS] because they are unavailable initially.

With the loss of secondary cooldown, the primary pressure increase to the opening setpoint of PSVs and the PSVs open automatically, which also leads to the continuous loss of primary coolant.

When the water level of SGs decrease to the “SG level (wide range) low 3” threshold, three trains of ASP [SPHRS] are actuated on “SG level (wide range) low 3 combined with ASG [EFWS] flow rate low continues 60 seconds” signal.

Finally, three trains of ASP [SPHRS] are used to remove the decay heat in the long term and the DEC-A final state is reached.

13.4.5.19.5 Analysis Assumptions

The detailed assumptions are presented in Reference [34]. The main assumptions are as follows:

a) The TLOCC with loss of secondary cooldown accident is assumed to happen at full power.

b) The ASG [EFWS] and VDA [ASDS] are both assumed to be unavailable during the accident analysis conservatively.

c) The initial state is at 102% nominal power, which maximises the primary heat.

d) The thermal design value is considered for the primary flowrate to penalise heat removal of the SG.

e) After the RT, a conservative decay heat curve (1.645σ uncertainties on the "B+C term") is used to represent the residual power history.

13.4.5.19.6 Results and Conclusions

The detailed results and conclusions for this accident are presented in Reference [34]. As results shown, the lowest water level that SGs reach is about 18% WR during the accident. The core remains covered during the whole accident progress. In the long term, the removal of core decay heat is ensured by the three trains of ASP [SPHRS].

The total consumption of ASP [SPHRS] tank water is about 2702.7 t with the heat removal via ASP [SPHRS] for 3 days. The total water inventory of ASP [SPHRS] tank is 3035 t. Thus, the water inventory of ASP [SPHRS] tank is sufficient to ensure the core heat removal via ASP [SPHRS] for 3 days.

13.4.6 DEC-A Source Term

Based on the selected DEC-A sequences in Table T-13.4-1, several fission product release paths are identified and discussed as below:

a) Fission products release to containment.

Sequences that result in fission products release to the containment, such as SB-LOCA, SBO and TLOFW, are bounded by the DBC Loss of Coolant Accident (LOCA) in Chapter 12, because of the more conservative assumptions in DBC LOCA source term analysis [35].

b) Fission products release to secondary side.

For the sequences that result in radioactive coolant leak to secondary side, including multiple SG tubes rupture (10 tubes), MSLB with SGTR (SGTR) (1 tube) in the affected SG, and SGTR (1 tube) with VDA [ASDS] stuck open in the affected SG, radioactive nuclides are released directly to the environment. The amounts of released coolant in DEC-A SGTR sequences is larger than that of the DBC SGTR source term.

c) Fission products release to fuel building.

Sequences that result in radioactive steam release to fuel building, which is caused by the evaporation of spent fuel pool coolant, such as loss of three PTR [FPCTS] trains, are bounded by dropping of fuel assembly accident, which considers the gap release phase of fuel [36].

As discussed above, the selected sequences for the DEC-A source term analysis are listed below:

a) Multiple SG tubes rupture (10 tubes).

b) MSLB with SGTR (1 tube) in the affected SG.

c) SGTR (1 tube) with VDA [ASDS] stuck open in the affected SG.

13.4.6.1 Multiple SG Tubes Rupture (10 tubes)

Multiple SG tubes rupture results in radioactive coolant leaking to secondary side via the ruptured tubes. The break leakages induce the contamination of the secondary side, then the radioactive coolant discharges to the environment via VDA [ASDS].

13.4.6.2 MSLB with SGTR (1 tube) in the Affected SG

The break of the main steam line is located in the downstream of MSIV. SGTR in the affected SG induces uncontrolled discharge of radioactivity to the environment. The release of source terms is terminated until the MSIV is isolated successfully.

13.4.6.3 SGTR (1 tube) with VDA [ASDS] Stuck Open in the Affected SG

SGTR leads to the loss of primary coolant, and the stuck VDA [ASDS] leads to uncontrolled discharge of radioactivity to the environment until the complete depressurisation of RCP [RCS].

13.4.6.4 Method of Analysis

13.4.6.4.1 Calculation Input

13.4.6.4.1.1 Primary Coolant Source Term

It is assumed that the reactor is in normal operation with fuel rods defecting before accident, and initial primary coolant activity is equivalent to { } in the stable state [37].

13.4.6.4.1.2 Thermal Hydraulic Input

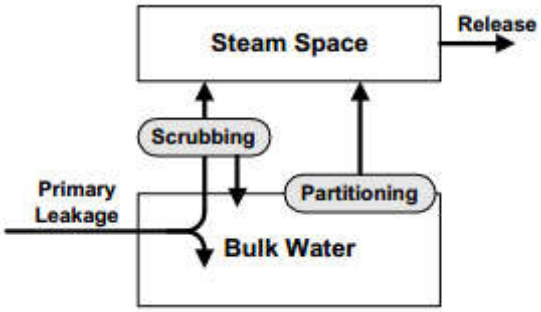
The thermal hydraulic input of DEC-A source term analysis is given in Sub-chapter 13.4.5.

13.4.6.4.2 Calculation Model and Assumption

13.4.6.4.2.1 Transport Model

All noble gas radionuclides released from the primary system are assumed to be released to the environment without reduction or mitigation [38].

The transport model of iodine and particulates which are released from the steam generators is shown in F-13.4-1.



F-13.4-1 Source Term Transport Model [38]

13.4.6.4.2.2 Leakage

The primary to secondary side leakage of the unaffected SG is assumed to be 44 L/h, which is the limiting leakage rate for the normal operation condition.

The break flow rate of the affected SG is derived from thermal hydraulic input.

13.4.6.4.2.3 Flash

A portion of the primary-to-secondary leakage will flash to vapour, based on the thermodynamic conditions in the reactor and secondary coolant [38].

a) During periods of steam generator dry out, the entire primary to secondary side leakage is assumed to flash to vapour.

b) With regard to the unaffected steam generators used for plant cool down, the primary to secondary side leakage can be assumed to mix with the secondary water without flashing during periods of tube fully submerged.

13.4.6.4.2.4 Scrubbing and Partitioning

If the secondary water level is high enough to fully submerge the tubes, the leakage that immediately flashes to vapour will rise through the bulk of the water and enter the steam space of the SG.

Scrubbing is credited during periods of total submergence of the tubes. The retention of particulate radionuclides in the SG is limited by the moisture carryover (0.25%) from the SGs [38].

The rate of the radioactivity that becomes vapour in the bulk water is assumed to at a rate of a function of the steaming rate and the partition coefficient, where the partition coefficient for elemental iodine is assumed to be 100 [39].

13.4.6.4.2.5 Chemical forms

Iodine releases from the steam generators to the environment are assumed to be 97% elemental and 3% organic [33].

13.4.6.5 Results

The DEC-A source terms results including the release time, and radioactivity of nuclides are the inputs of radiological consequences analysis.

The results have been presented in DEC-A source terms analysis report [40].

13.4.7 Radiological Consequences of DEC-A

The evaluation of DEC-A radiological consequences will demonstrate that the requirements of RPTs defined in the generic safety requirements are met [41]. The introduction for the methodology and assumptions of the evaluation of DEC-A radiological consequences is same as DBA which is presented in PCSR Sub-chapter 12.11.2 and 12.11.4.

13.5 DEC-B Analysis

13.5.1 Introduction of DEC-B Scenarios

The definition of severe accident stated in Safety Assessment Principles (SAPs) is based on numerical targets of radiological consequences [42]. Technical Assessment Guide (TAG) T/AST/007 states that: “An event that could reasonably exceed any of these numerical targets is potentially a severe accident and should be considered in the safety case.” To meet these principles, the resultant event is termed a Severe Accident (SA) or DEC-B event, if the continuous loss of coolant or secondary heat sink leads to core or spent fuel uncovering and consequently melting of the core or spent fuel.

To achieve the safety objectives mentioned in Sub-chapter 13.2, the basic strategy of severe accident mitigation is to maintain the integrity of the containment in both short and long term as far as possible.

Some severe accident sequences or phenomena are identified as practically eliminated, such as fuel melt scenarios in SFP and containment isolation failure (see PCSR Sub-chapter 13.5.8). However, the integrity of the containment can be challenged by various phenomena and threats that occur during a DEC-B event. To provide cooling to the melted core material (“corium”) and maintain the integrity of the containment, severe accident mitigation measures have been developed for the Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) which forms the basis for severe accident mitigation in the UK HPR1000 design [43], [44].

The overall objective of SAA is to prove that the nuclear safety risks from severe accidents are tolerable and ALARP along with the PSA. CGN consider practical elimination as an objective to limit large or early radiological release, which will also support the ALARP demonstration.

The golden thread of the SAA safety case is presented in F-13.5-1, which shows the overall logic of SAA and interaction with other aspects of design.

In the topic area of SAA, the framework is as follows:

1) Severe accident sequences identification:

Based on the reference design and general safety requirements, potential sequences with core melt or significant radiological release need to be identified. For the UK HPR1000, the selection method of a severe accident list is combining the probabilistic and deterministic methods with rational engineering judgements. This approach ensures that no remarkable risk is omitted.

2) Severe accident phenomena understanding:

The physicochemical and radiological phenomena in severe accidents are very complicated and occur in various stages of the severe accident progression. However, the generic features of severe accident progression show their consistency since they are mainly dominated by physical processes related to the fuel degradation. After a review of the identified SA sequences and potential accident progression, the phenomena of concern are selected. Sequence analysis needs to be performed to confirm the correctness if necessary. Some severe accident phenomena may be excluded based on international consensus and justification in the UK HPR1000.

3) Severe accident management strategy determination:

The overall severe accident management strategy for the reactor is to maintain as many barriers between the core and the environment as possible for as long as possible. This means to prevent RPV failure and containment failure or if this cannot be avoided, to avoid failure at high pressure and to delay failure for as long as possible. Strategies are derived to cope with the phenomena that threaten barriers integrity. CGN's experience in previous projects, relevant good practice and lessons learnt from Fukushima accident also contribute to the basis and source of the strategy. The general structure of SAMG is outlined and a detailed SAMG will be ready in site licensing stage.

4) Severe accident mitigation system design:

Based on strategies determined, severe accident mitigation systems need to be designed step by step.

Firstly, safety functional requirements are derived from strategy. The initiatory configuration of system is based on CGN's experience in previous projects, relevant good practice and lessons learnt from Fukushima accident. Severe accident analysis is performed to determine or confirm the capacity of equipment and time allowance for operator action. During this process, requirements on categorisation & classification, equipment qualification, I&C, electrical engineering, structure integrity, human factors (operator action and human accessibility), and civil engineering should be considered. Specific requirements identified for each system are included. This is the basis of the design of SSCs.

SAA will evaluate the performance of the engineered mitigation measures and thereby show that these measures are effective in mitigating the identified phenomena and scenarios. The principles and guidance from the International Atomic Energy Agency (IAEA) and Western European Nuclear Regulators' Association (WENRA) relevant to SAA are followed. SA codes used are all well-validated and their applicability to the UK HPR1000 is assessed. To show the absence of cliff-edge effects or to determine the margin to a cliff-edge effect, sensitivity studies on key parameters, analysis assumptions, and manual actions will be performed in SAA.

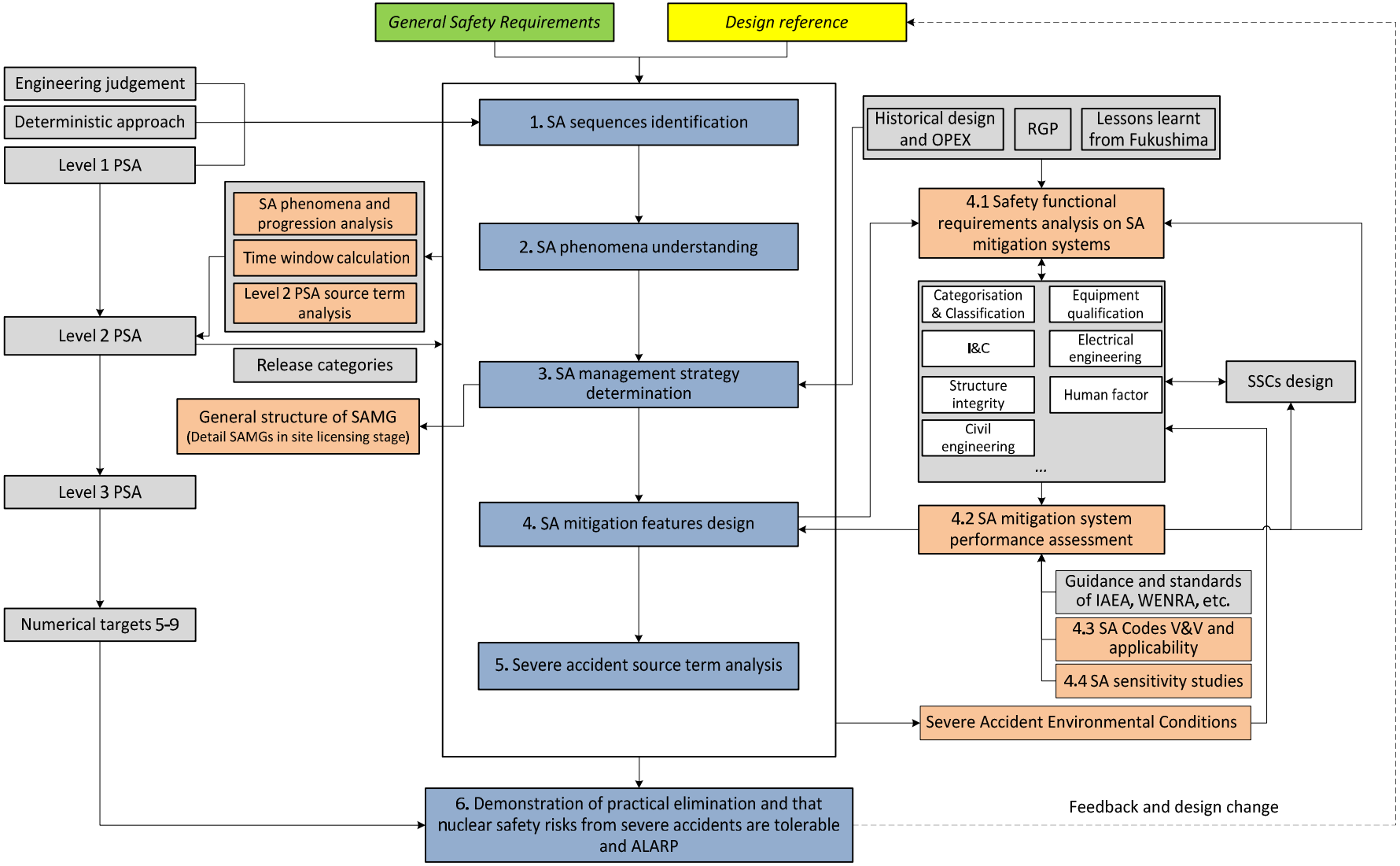
During this process, shortfalls or improvements in the design may be revealed to provide feedback to SSCs design.

5) Severe accident source term analysis:

Severe accident source term analysis is performed to determine the possible consequence under severe accident condition. Possible release path and behaviour of fission products are considered. This provides an input to the equipment qualification, and human accessibility assessment.

Severe accident environmental conditions in the containment are derived to provide an input to equipment qualification, human accessibility assessment, and ultimate strength assessment of the internal containment.

Based on all activities above, a review can be performed to evaluate whether sequences that would lead to an early or large radioactive release are practically eliminated. An ALARP demonstration regarding SA mitigation systems need to be presented. Feedback and potential design changes to the reference design may be identified.



F-13.5-1 Golden thread of SAA safety case

13.5.2 Selection of Representative DEC-B Events

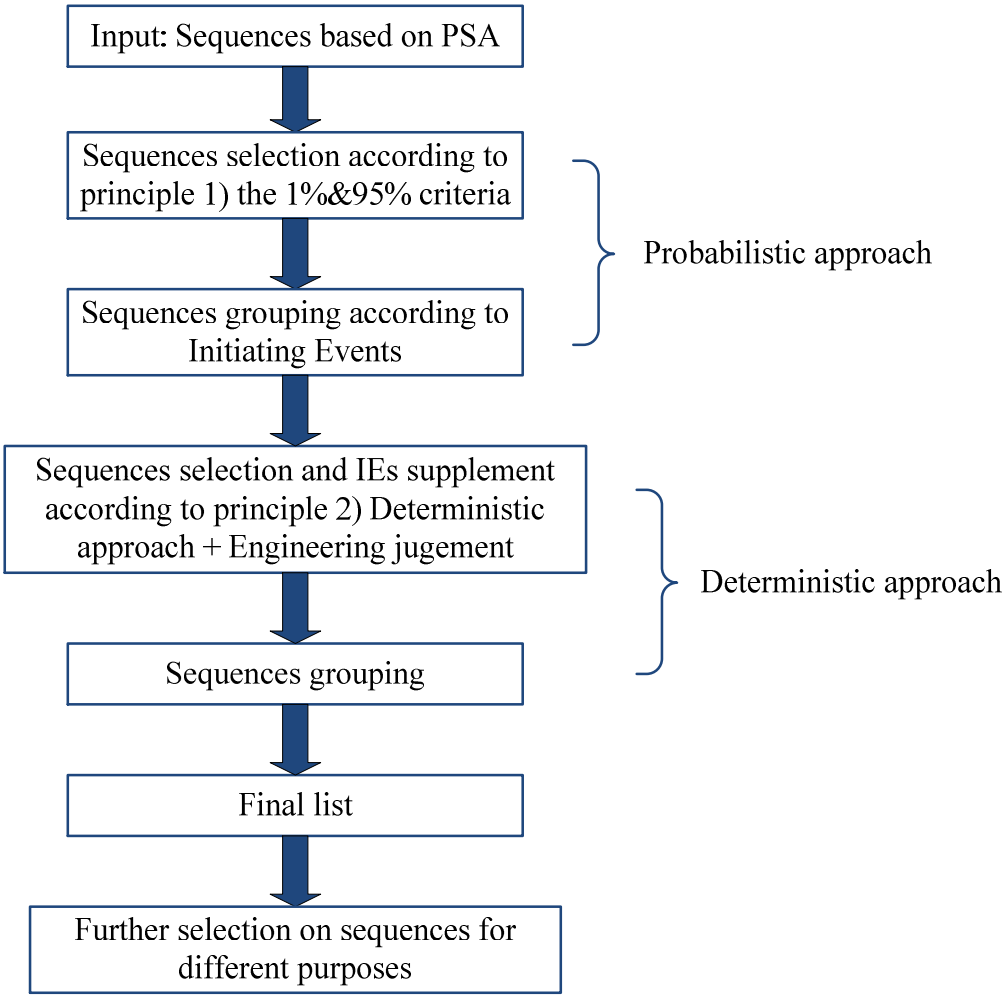
13.5.2.1 Principles and Methods

In general, the method of selecting the severe accident sequences for the UK HPR1000 combines the probabilistic assessment and deterministic methods with rational engineering judgements. The specific selection principles of typical severe accident sequences are shown as follows [45]:

a) According to the Level 1 PSA results, the dominant accident sequences with frequencies exceeding 1% of the total Core Damage Frequency (CDF) shall be selected, or if the sum of all selected accident sequence frequencies accounts for 95% of the total CDF.

b) The final severe accident sequence selection shall fully consider the impact of different initiating events on the accident scenarios.

The input for severe accident sequence screening is the complete level 1 PSA sequences including at-power, low power and shutdown states in the reactor core as well as the spent fuel pool. The whole process as shown in F-13.5-2 includes the main steps of probabilistic screening, deterministic screening and the selection on sequences for severe accident mitigation systems assessment. The final list for severe accident analysis will be derived after probabilistic screening and the deterministic screening step. The accident sequences for different mitigation measures assessment should be selected based on the above final sequence list considering the different objectives of each system to ensure the selected sequences are the bounding ones.



F-13.5-2 Process of severe accident sequence selection

13.5.2.2 Severe Accident Sequences List Identification

In this section, the representative severe accident sequences of the UK HPR1000 are selected based on the internal events Level 1 PSA results. The selection method combines the probabilistic and deterministic methods with rational engineering judgements.

13.5.2.2.1 Selection Based on Probabilistic Method

13.5.2.2.1.1 Selection based on First Principle

According to the first selection principle in Sub-chapter 13.5.2.1, the Level 1 PSA results of the UK HPR1000 are analysed to determine the dominant sequences. All operating states listed in Table T-13.5-1, such as at-power, low power and shutdown, are analysed in the internal events Level 1 PSA of the UK HPR1000. All the sequences of which the total sequence exceeds 95% of the total CDF are screened in the severe accident the sequence list. It is shown that this list covers not only all the sequences of which the sequence exceeds 1% of the total CDF but also some of the sequences of which that is less than 1%.

13.5.2.2.1.2 Preliminary grouping from PSA perspective

In Sub-chapter 13.5.2.2.1.1, 50 severe accident sequences are selected preliminarily based on the probabilistic method in which 33 of them are in power condition, while 17 of them are in shutdown condition. This list should be grouped according to initiating events and system functions with the following criteria: 1) If the sequences have the same initiating events, they could be grouped. 2) If the different faults from the PSA lead to the same system function failure, they could be grouped. For example, the failure of feed-bleed includes failure of feed-bleed systems and human errors, hence, these two sequences could be grouped. In the UK HPR1000, the above 50 accident sequences selected are grouped into 12 categories including 26 sequences shown as T-13.5-2.

13.5.2.2.2 Selection Based on Deterministic and Engineering Judgements

According to the second selection principle in Sub-chapter 13.5.2.1, the final severe accident sequence selection shall fully consider the impact of different initiating events on the accident progression. For those sequences with low frequencies screened out by PSA but high consequence, they should be supplemented from the deterministic assessment and engineering judgements.

Comparing with the initiating events from the Level 1 PSA, sequences of loss of main feedwater in Plant Operating State (POS) A, LOOP in POS A, Interfacing Systems Loss of Coolant Accident (ISLOCA), and cold overpressure are left out because of the low frequencies. However, the sequences of loss of feedwater and LOOP in POS A are supplemented by the deterministic analysis and engineering judgements.

The complete preliminary SAA list contains sequences shown in Table T-13.5-2 from PSA and the supplemented ones above, which can be grouped by deterministic assessment in this step. The main principle of grouping is that for accidents sequence with the same or similar progression rates, the one with more severe consequence bounds the other ones.

The severe accident sequences of the SGTR category can be grouped into the SB-LOCA category. The SLB+SGTR is not considered in the final SAA list because it leads to containment bypass which is stressed in Level 2 PSA.

Sequences of loss of feedwater in POS A can bound the similar sequence of loss of cooling chain and loss of residual heat removal in POS C based on the deterministic analysis and engineering judgements.

Sequences of LOOP in POS A can bound the similar sequences of LOOP in POS C and loss of 10kV SBO Power Distribution System in POS A based on the deterministic analysis and engineering judgements.

The progression of loss of residual heat removal and LOOP in POS D are similar, so they are grouped into loss of residual heat removal in POS D.

For the ATWS sequence "POS A, LOMFW, RT signal fails and core damage" in T-13.5-2, it means all the signal cannot be sent correctly and there is no mitigation measure, so it is filtered out of the list for the severe accident analysis.

For the boron dilution events in POS A, boron dilution with ATWS and SLB with ATWS, they are also conservatively considered in the PSA model, therefore, they are filtered out of the list as well.

The SLB sequence selected from the PSA is considered conservatively as core damage in the Level 1 PSA model. It can be bounded by the ATWS sequence as shown in Table T-13.5-3. Therefore it is filtered out of the list.

Based on the above analysis, the final list of severe accidents after grouping includes 7 categories and 7 accident sequences in total as shown in Table T-13.5-3. The sequences to be analysed for different objectives can be selected from the final list.

13.5.2.2.3 Accident Sequence Selection for Different Mitigation Measures Assessment

For the assessment of severe accident mitigation measures described in PCSR Chapter 13.5.5, bounding accident sequences are selected starting from T-13.5-3. Conservative assumptions are adopted for different analysis objectives because of different severe accident phenomenon procession. For the assessment of different severe accident mitigation measures, the bounding sequences are selected as shown in T-13.5-4.

T-13.5-1 Plant Operating States Analysed in UK HPR1000

POS	Standard Operating Conditions	RCP [RCS] State	Coolant Inventory
A	Reactor in power	closed	PZR level is at set point
	Hot standby	closed	PZR level is at set point
	Hot shutdown	closed	PZR level is at set point
	Intermediate shutdown with Normal Shutdown with Steam Generators (NS/SG) connection conditions (P≥130 bars abs)	closed	PZR level is at set point
B	Intermediate shutdown with NS/SG connection conditions (P<130 bars abs)	closed	PZR level is at set point
	Intermediate shutdown with RIS-RHR connection conditions	closed	PZR level is at set point
C	Intermediate shutdown with RIS-RHR	closed	PZR level is at set point or full
		closed	
	Normal cold shutdown (RCP [RCS] pressurisable)	Non-closed and	≥ 3/4 loop level

POS	Standard Operating Conditions	RCP [RCS] State	Coolant Inventory
		pressurisable	
D	Normal cold shutdown for maintenance (RCP [RCS] not pressurisable)	Non-closed and not pressurisable, Reactor cavity non fillable	≥ 3/4 loop level
		Non-closed and not pressurisable Reactor cavity fillable	
E	Normal cold shutdown for refuelling		Reactor cavity flooded
F	Core totally unloaded	-	-
G_1	Normal cold shutdown for maintenance (RCP [RCS] not pressurisable)	Non-closed and not pressurisable, Reactor cavity non fillable	Around 3/4 loop level

1: Where POS G is a special plant operating states during POS C and POS D, in which the reactor coolant inventory is near the mid-loop water level. It brings additional risk and need to be considered separately.

T-13.5-2 Preliminary SAA List from PSA Results

SN	Category	Sequence description
1	SB-LOCA	POS A, SB-LOCA, medium pressure rapid cooldown failure, feed and bleed fails and core damage
		POS A, SB-LOCA, MHSI fails, LCD succeeds, but LHSI fails and core damage
		POS B, SB-LOCA, MCD failure and core damage.
		POS C, SB-LOCA, MHSI fails, RHR recovery succeeds, secondary cooldown fails and core damage
2	SGTR	POS A, single-tube SGTR, MCD succeeds, isolation of SG succeeds, MHSI fails, LCD fails and core damage.
		POS B, single-tube SGTR, MCD succeeds, isolation of SG succeeds, secondary cooldown succeeds, MHSI fails, LCD fails and core damage.
3	ATWS	POS A, LOMFW, RT signal fails and core damage.
		POS A, ATWS with loss of main feedwater, Turbine Trip succeeds, RCP [RCS] Pumps trip succeeds, PSV open succeeds, RBS [EBS] succeeds, secondary cooldown failed and core damage.

SN	Category	Sequence description
		POS A, ATWS with LOOP, 2 and more than 2 control rods stuck outside of the core, EDG succeeds, PSV Re-closure succeeds, secondary cooldown fails and core damage.
		POS B, ATWS with SLB at downstream MSIV, two or more control rods stuck outside of the core and core damage.
		POS A, Homogeneous boron dilution, automatic dilution source isolation fails, two or more control rods stuck outside the core and core damage.
4	Loss of cooling chain	POS A, LOCC, PSV Re-closure succeeds, no RCP [RCS] pump seal LOCA, MCD fails and core damage.
		POS C, LOCC, RHR Safety Valve open succeeds and close succeeds, secondary cooldown fails and core damage.
		POS G, loss of heat sink, water supply failure of LHSI system, core being damaged after the water is vaporised to dryness.
5	RPV break	POS A, RPV broken, no mitigation measures, and core damage
6	SLB + SGTR	POS A SGTR, MCD succeeds, isolation of SG fails and core damage.

SN	Category	Sequence description
7	IB-LOCA	POS A, Intermediate Break - Loss of Coolant Accident (IB-LOCA), MCD succeeds, MHSI fails and core damage.
8	Loss of residual heat removal	POS C, LORHR, RHR Safety Valve open succeeds and close succeeds, secondary cooldown fails, Feed and Bleed succeeds, MHSI fails and core damage.
		POS D, LORHR, MHSI fails, LHSI fails and core damage.
9	Loss of power	POS A, PSV Re-closure succeeds, there is no RCP [RCS] pump seal LOCA, SBO succeeds, secondary cooldown succeeds, LCD fails and core damage.
		POS C, LOOP, EDG fails, SBO DG succeeds, RHR succeeds, RHR Safety Valve open succeeds and close succeeds, secondary cooldown (including ASG [EFWS] and VDA [ASDS]) fails and core damage
		POS D, LOOP, EDG and SBO DG failed to be started, and core damage
10	LB-LOCA	POS A, Large Break - Loss of Coolant Accident (LB-LOCA), accumulator is unavailable and core damage.
11	Boron dilution	POS A, Homogeneous boron dilution, automatic dilution source fails, the reactor trip succeeds, manual dilution source isolation fails and core damage.

SN	Category	Sequence description
12	SLB	POS A, SLB, MSIV Up-Stream, all Control Rod Insertion succeeds, not induce SGTR, Isolation of MSIV succeeds, Isolation of Main Feedwater succeeds, RBS [EBS] succeeds, secondary cooldown fails and core damage.
		POS A, Main Steam Line Break (MSIV Up-Stream), RT succeeds, not induce SGTR, Isolation of MSIV succeeds, isolation of Main Feedwater fails and core damage.
		POS B, SLB downstream MSIV, isolation of MSIV fails and core damage.

T-13.5-3 Final SAA List

SN	Category	Sequence after merging	Description
1	SB-LOCA	POS A, SB-LOCA, medium pressure rapid cooldown failure, feed and bleed not implemented in time, MHSI failed to be put into operation, and core damage	From PSA, merging POS A , B and C, and enveloping them with POS A. The same SGTR sequence is bounded. The two sequences of POS A in T-13.5-2 can also be grouped because of the similar progressions.
2	LB-LOCA	POS A, LB-LOCA, MHSI and LHSI failure and core damage	Supplementation based on deterministic and engineering judgements, bounding the LB-LOCA sequence selected from PSA.
3	IB-LOCA	POS A, IB-LOCA, MHSI and LHSI failure, and core damage	Based on sequence selected from PSA and conservative assumption is considered through the deterministic and engineering judgements.
4	ATWS	POS A, loss of main feedwater, all the control rods being stuck outside of the reactor core, RBS [EBS] success but secondary cooling failure and core damage	Based on sequence selected from PSA and conservative assumption is considered through the deterministic and engineering judgements. Bounding the similar sequence of ATWS with LOOP selected form PSA.

SN	Category	Sequence after merging	Description
5	Loss of feedwater	POS A, total loss of feedwater, feed and bleed operation not implemented in time, and core damage	From deterministic perspective. The similar sequence of loss of cooling chains from the PSA can be bounded. Loss of residual heat removal and loss of cooling chains in POS C from the PSA can be bounded.
6	LOOP	POS A, LOOP, EDG and SBO DG failed to be started, and core damage	For LOOP, since the core damage frequency is very low, sequences related to POS A LOOP cannot be identified from the PSA perspective. According to the deterministic method and engineering judgement, from the severe accident perspective, POS A, LOOP+EDG failure + SBO DG failure can envelope the sequences related to conditions POS C.
7	Loss of residual heat removal	POS D, loss of residual heat removal, MHSI failure, LHSI failure and core damage.	Based on the sequence selected by the PSA, merging loss of LOOP and loss of residual heat removal in POS D.

T-13.5-4 Accident Sequence Selected for the Different Severe Accident Mitigation Measures Assessment

No.	Severe accident mitigation measures	Severe accident sequence category	Severe accident sequence description
1	EUH [CCGCS]	SB-LOCA	POS A, SB-LOCA accident, MHSI and LHSI failure and core damage
		IB-LOCA	POS A, IB-LOCA, MHSI and LHSI failure and core damage
		LB-LOCA	POS A, LB-LOCA, MHSI and LHSI failure, and core damage
		LOOP (SBO)	POS A, LOOP, EDG and SBO DG failed to be started, and core damage
2	SADV	ATWS	POS A, loss of main feedwater, all the control rods being stuck outside of the reactor core, RBS [EBS] success but secondary cooling failure and core damage
		SBO	POS A, LOOP, EDG and SBO DG failed to be started, and core damage
3	EHR [CHRS]	LB-LOCA	POS A, LB-LOCA, MHSI and LHSI failure and core damage
4	IVR	LB-LOCA	POS A, LB-LOCA, MHSI and LHSI failure, and core damage

No.	Severe accident mitigation measures	Severe accident sequence category	Severe accident sequence description
		IB-LOCA	POS A, IB-LOCA, MHSI and LHSI failure and core damage
		SB-LOCA	POS A, SB-LOCA, MHSI and LHSI failure and core damage
		ATWS	POS A, loss of main feedwater, all the control rods being stuck outside of the reactor core, RBS [EBS] success but secondary cooling failure and core damage
		SBO	POS A, LOOP, EDG and SBO DG failed to be started, and core damage
5	EUF [CFES]	LB-LOCA	POS A, LB-LOCA, MHSI and LHSI failure and core damage

13.5.3 Potential Severe Accident Progression without Mitigation Measures

The physicochemical and radiological phenomena in severe accidents are very complicated and occur in various stages of the severe accident progression [46]. However, the generic features of severe accident progression show their consistency since they are mainly dominated by physical processes related to the fuel degradation. Severe accident progression with related phenomena consists three phases:

1) In-core phase.

In-core phase is the period from the initial event to the failure of the lower support plate or core barrel, covering associated phenomena, for instance, the exposure, heat-up and degradation of the core and relocation into lower head.

Initiating with a transient event, the primary system breaks or safety valves discharge lead to continuous loss of primary coolant and insufficient core cooling. If safety systems fail to supplement the coolant inventory, the reactor water level gradually decreases and the core is uncovered. The core is heated up due to the residual heat. With the high temperature of core, the zircaloy oxidation occurs which not only generates hydrogen but is also highly exothermic, thus further increasing the core temperature. The large amount of hydrogen release to containment may lead to hydrogen combustion or detonation which could challenge containment integrity. It is noted that the heat generation from zircaloy oxidation at high temperature may exceed the decay heat. The fuel assemblies, control rods and support structures in core regions begin to melt due to the decay heat and the heat of cladding oxidation. Fission products are released from the damaged core. The damaged core continues to melt and then falls into lower regions of the core. The molten materials of fuel and core structures, called corium, continuously heat up the lower support plate and other support structures, ultimately relocating in the lower plenum after the support plate fails. There are two relocation paths based on different phenomena, one is called downward relocation, which means the corium melts directly downwards through core-support structures to the lower head; the other is called sideward relocation, which means the corium melts through shroud and barrel then down into the lower head. The ultimate relocation path into the lower head depends on multiple factors including the power distribution in the core, the design of the core and surrounding structures and the thermo-hydraulic boundary.

2) Lower plenum phase.

Lower plenum phase is the period from the failure of lower support plate or core barrel to the RPV failure, covering associated phenomena, for instance, in-vessel Fuel Coolant Interaction (FCI), corium stratification, ablation effect and molten pool heat transfer (heat conduction, heat convection and heat radiation).

After the lower support plate failure, the corium relocates into the lower plenum. When the corium falls into the residual water pool of the lower plenum, the molten

corium may fragment into corium particles with rapid energy transfer which leads to rapid flash of the residual water, shock waves and possible mechanical damage. The phenomenon of this interaction is called in-vessel FCI (in-vessel steam explosion).

The molten corium, solidified during the relocation process, is called crust. Due to the difference of material densities, the corium pool in the lower plenum can develop into two layers:

a) An oxide layer (molten oxide corium with surrounded by solid crust) composed of all the core oxide fragments.

b) A molten metal layer at the tops of the crusts on the oxide layer consists of all components with the low density (reflector, core support plate, part of core barrel and lower internal structures) in the core area.

Two-layer stratified corium pool configuration has been observed in some experiments of international projects and investigated theoretically [47]. Based on the acquired knowledge, the two-layer model is widely used in the IVR effectiveness analysis and the relevant research. It is also widely adopted in the severe accident analysis codes. A molten pool having a three-layered structure was produced in a series of small and medium-scale tests performed in the MATERIAL SCALING (MASCA) program with iron and stainless steel as additional material [47]. It contains molten heavy metal at the bottom, molten oxides at the middle and molten light metal on the top. Although the three layer corium pool model is founded in the MASCA program, there are still many uncertainties associated with the three-layer model. According to the present analysis status of international research, the three-layer model will have a thinner lighter metallic layer and part of uranium will transform under the oxide layer. The heat transfer of the corium pool will change. The heat flux near the heavy layer may increase and the heat focusing effect near the metallic layer may be enhanced. At present, the international research on the three-layer model is ongoing with no international consensus drawn and the relevant progress will continue to be followed.

For the corium behaviour in lower plenum, the cooling of corium pool in the lower plenum might rely on the heat transfer through the potential gaps between solid crusts and RPV wall. For this potential phenomenon, the influence is described as follows. When there is water present in the lower plenum, the residual water flows into the gaps and maintain the heat transfer between the crusts and vessel wall, therefore corium cooling is ensured. When there is no water or the water runs out in the lower plenum, the layer of solid crusts begins to melt again due to the residual heat, resulting in the increase of corium materials temperature and the heat-up of the vessel lower head. If no additional water is added to the vessel, the corium continues to heat, ultimately leading to the RPV lower head failure.

3) Ex-vessel phase.

Ex-vessel phase is the period after RPV failure, covering associated phenomena, for instance high pressure melt ejection and Direct Containment Heating (DCH), ex-vessel FCI and Molten Core-Concrete Interaction (MCCI).

When RPV failure occurs, the mode of corium release from failure opening is largely dominated by RPV primary pressure. If the primary pressure is similar or slightly higher than the containment pressure, the molten corium will fall into the reactor pit due to the gravity. This may lead to MCCI which will not threaten the integrity of the containment in the short term. If the primary pressure is much higher than the containment pressure, High Pressure Melt Ejection (HPME) will occur. In this scenario, the molten corium is ejected into the reactor pit and then transported into the containment in form of the fragmented corium droplets. In this process, the molten metal in the corium is oxidised by the steam with hydrogen and heat generated. The heat transfer between the corium droplets and the gas in containment is rapid and sufficient, which leads to the quick increase of containment temperature and pressure. The high temperature of the fragmented corium droplets or the hot gases can also lead to the combustion of hydrogen generated during HPME and previous severe accident progression, increasing the containment pressure as well. This whole process including the complex phenomena mentioned above is called DCH, which threatens the integrity of containment and leads to early containment failure.

When the corium falls into the cavity after RPV fails, it interacts with the coolant in cavity if the cavity is flooded resulting in the phenomenon ex-vessel FCI (steam explosion). The generated steam and shock wave may threaten the integrity of the containment and lead to containment failure. Another interaction occurring when the corium is ejected or falls into the reactor pit is MCCI. When the molten corium contacts with the concrete, the decay heat of fission products in the corium transfers to concrete and the thermal degradation and chemical reaction begins, leading to the generation of substantial non-condensable and combustible gas such as H_2. The gas mixture is released and accumulated in the containment, raising the risk of containment overpressure. Furthermore, the accumulation of the combustible gas can lead to combustion or even explosion which can seriously threaten the integrity of containment in the long term. If the base is continuously corroded, the radioactive substances can be released directly to the environment underground and then potentially transported further by the groundwater, therefore the integrity of the containment cannot be maintained.

13.5.4 Key Phenomena of Severe Accidents Considered To Date

A list of accident phenomena has been compiled and assessed for the HPR1000 (FCG3) and for the GDA to date; these are discussed in the sub-sections below. To ensure that this list is complete, a systematic approach will be used to identify any further severe accident phenomena to consider in the GDA. Firstly RGP from a number of sources will be reviewed to determine which phenomena have been

considered elsewhere. Secondly, any specific features of the UK HPR1000 that could conceivably lead to phenomena not considered elsewhere will be assessed and if any, added to the list. The final list will be reviewed to determine if any phenomena can be excluded and if so justification for the exclusion made.

13.5.4.1 High Pressure Melt Ejection and DCH [48]

In some scenarios, a failure of the RPV at a high pressure which greatly exceeds containment pressure might occur and lead to HPME. When HPME occurs, the molten corium is ejected into the cavity at a high velocity and is then fragmented into corium droplets by the gas flow. The fragmented corium droplets are then transported from the cavity to the containment. As partial liquid metal in the molten corium may be oxidised by steam, which will generate hydrogen and heat released into the containment. Furthermore, hydrogen combustion would also produce heat in the containment. Due to consideration of the large surface area per volume for the corium droplets, heat transfer from the corium to the gas of the containment is significant. All these factors would cause the pressure and temperature of containment to increase rapidly, which might lead to containment failure.

13.5.4.2 Hydrogen Combustion [49]

For a nuclear power plant with a pressurised water reactor, most of the hydrogen sources for the UK HPR1000 are generated from zirconium oxidation during severe accidents. With the exposure of high temperature fuel to steam, the zirconium cladding will react with water vapour to produce hydrogen and release heat. The reaction can be described as follows:

$$Zr + 2H_2O \rightarrow 2H_2 + ZrO_2 + heat$$

The heat released from this reaction will elevate the temperature of the fuel cladding and in turn accelerate the reaction rate. This reaction tends to be quick and cannot be stopped until the fuel clad is isolated from the oxidant. For a typical accident scenario, a few hundred kilograms of hydrogen could be generated during the in-core process.

If the RPV fails, molten core debris will contact with concrete and produce combustible gases either through thermal degradation or through chemical reactions. Once hydrogen is released into the containment, the hydrogen mixes with the atmosphere in the containment which leads to flammable mixtures. Hydrogen combustion or detonation may occur and cause high pressure spikes and high temperature loads, which will threaten the integrity of containment.

There are three different combustion modes which will lead to different consequences for the containment:

a) Diffusion flame

Diffusion flame is a steady combustion and it is usually formed at the outlet of the

hydrogen jet. This is usually the case if there is ignition at the outlet of the hydrogen jet.

b) Deflagration

Deflagration is combustion of a premixed combustible gas cloud with a slow flame velocity. In deflagration mode, the flame propagates at a subsonic speed relative to the unburned gas. For deflagration combustion in an unobstructed and unconfined space, the deflagration is not likely to accelerate; the pressure rise in this case is moderate. However, if there is an obstruction along the flame progress, the deflagration flame tends to be accelerated by the turbulence effect and it is possible to transfer to detonation. In this case, the resultant pressure may become significant. Deflagration combustion is common and requires detailed analysis in the assessment of consequences of combustion.

c) Detonation

Detonation is a quick combustion with a flame speed higher than the speed of sound and the shock wave tends to form ahead of the flame. There are two schemes that will lead to detonation. The first scheme is direct detonation. Not only high hydrogen concentration and stoichiometric gases, but also high activation energies are required to initiate direct detonations. The second scheme is Deflagration to Detonation Transition (DDT), which has been described in the ‘deflagration’ section.

13.5.4.3 MCCI [50]

The corium will relocate into the lower head and form the debris bed or corium pool when the reactor core is insufficiently cooled during severe accidents. Melt-through failure or creep failure of the lower head may happen if the decay heat of the debris bed can’t effectively be removed from the lower head. The high-temperature corium erupts into the reactor pit through breaks on the lower head and interacts with the concrete leading to the complicated physicochemical reactions called MCCI, described previously. Consequently, a large amount of non-condensable gas is produced, leading to an increase of the containment pressure which threatens the integrity of the containment. The hydrogen released into the containment may increase the risk of hydrogen detonation. Meanwhile, the concrete pedestal is continuously damaged by the melt, which finally leads to radioactive leakage if melted through.

The IVR strategy can prevent MCCI by avoiding RPV failure with a high level of confidence based on the demonstration presented in Sub-chapter 13.5.6.3. The details of the MCCI analysis will be described in the Level 2 PSA report considering the possible RPV failure.

13.5.4.4 Steam Explosion

The steam explosion can be classified into two categories, in-vessel steam explosion

and ex-vessel steam explosion, according to the location where the steam explosion occurs.

13.5.4.4.1 In-vessel steam explosion

During severe accidents, in-vessel steam explosion may be possible as the lower head still has water inside when the corium begins to relocate. The shock wave caused by the steam explosion may break the RPV wall and eject the fragments to the containment at a high velocity, threatening the integrity of the containment. In addition, in-vessel steam explosions may also lead to corium leakage, causing an ex-vessel steam explosion or MCCI which may also threaten the containment integrity.

Several mechanism experiments and international projects have been launched to study in-vessel steam explosion. Some international projects, such as Steam Explosion Review Group (SERG) [51] and SERENA [52][53], have been launched to figure out the risk of In-Vessel Steam Explosion. The results of this research show that in-vessel steam explosion can be excluded from consideration. The detailed reasons are listed below:

a) Firstly, the possibility of triggering in-vessel steam explosion is very low.

Several experiments, such as KROTOS, FARO and MIXA, have been carried out internationally to analyse the mechanism of steam explosion. These experiments point out the phenomena as follows:

- Without external triggering, it is unlikely for the steam explosion to happen spontaneously [54][55][56].
- Saturated water will suppress the steam explosion [57].
- Compared to other materials, it is difficult for the prototype corium to trigger steam explosion [55][56][58].

All these experiments support the conclusion that: The condition for triggering in-vessel steam explosion is very rigorous, the possibility of in-vessel steam explosion is very low. A particular case is the TMI-2 accident where no steam explosion happened [46].

Besides the conclusions drawn from the experiments, the SERG project also has the similar points of view. The research shows that to trigger a steam explosion, the following conditions must be met [51]:

1) Sufficient reaction material. Steam explosion need sufficient corium (tens of tons) poured into the lower head in the short premixing stage and also sufficient cooling water. At the beginning of relocation, the mass of corium is very low. At the same time, the water level decreases sharply with the increase of relocations. The corium and water cannot match the needed conditions at the same time.

2) Sufficient premixing. The steam explosion needs sufficient heat transfer area. The diameter of fragments must be within a suitable range. If the diameter is too small, the fragments will be frozen quickly, if the diameter is too large, the heat transfer is low.

3) Suitable triggering. There must be some pulse to trigger the steam explosion. According to the experiments, without triggering, the probability of steam explosion is very low.

4) Suitable void fraction. The void fraction cannot be too large. Stable vapour film produced by saturated water will prevent the triggering. The temperature and pressure will affect the void fraction.

The research of the SERG project shows that to meet all these conditions is physically impossible, or at least of very low probability [51], this further confirms the conclusion that the condition for triggering in-vessel steam explosion is very rigorous, the probability of in-vessel steam explosion is very low.

b) Secondly, the RPV failure due to the pressure of in-vessel steam explosion is very unlikely.

In-Vessel Steam Explosion is sufficiently studied in the deterministic analysis. In the SERG project, there is a consensus among the experts that research on FCI has been successful in resolving the alpha mode of containment failure (early containment failure resulting from an in-vessel steam explosion) from the risk perspective.[51]

In the SERENA project, calculations were performed by using ESPROSE-m, IDEMO, IFCI, IKEMIX, JASMINE, MATTINA, MC3D, PM-ALPHA, TEXAS-V, TRACER, VAPEX and VESUVIUS codes. Despite the large differences on the hypotheses, approaches, models, parameter setting philosophies and geometrical representations, no critical events with respect to reactor safety were predicted, especially for the in-vessel case with respect to lower head failure [52][53].

c) Thirdly, the conclusion of SERENA project is applicable for the UK HPR1000.

The SERENA project uses generic cases, independent from reactor types and designs. There is a generic situation that was considered by all participants as a bounding case for FCI in reactor conditions, regardless of the reactor type and design of the light water reactor. This generic situation assumes that the steam explosion occurs at a moment during the penetration of a large amount of core melt into a pool of water.

When combining all the partners' interest for in-vessel FCIs, the one of most concern for in-vessel FCI among the plausible scenarios of in-vessel melt progression is that a gravity pour of UO_2-ZrO_2 melts in the lower head in a 2-m-deep pool of saturated water at moderate system pressure. Both single and multi-pours are of concern [51].

The in-vessel steam explosion phenomena of all light water reactors are similar. The

analysed cases of SERENA are independent of reactor type and design. The interaction model, material, water level, temperature of corium, pressure and the radius of the RPV in the UK HPR1000 are similar to the cases in the SERENA. The conclusion of SERENA is suitable for light water reactors, including the UK HPR1000.

As discussed above, it could be concluded in-vessel steam explosions can be excluded from the SAA for the UK HPR1000, because firstly, the probability of triggering in-vessel steam explosion is very low and secondly, the RPV failure due to the pressure load of in-vessel steam explosion is very unlikely.

13.5.4.4.2 Ex-vessel steam explosion

This scenario assumes that the corium falls down to the reactor pit when the RPV is melted through. The high temperature corium will contact with the cooling water, generating a large amount of steam in a short period of time, forming a pressure pulse, or causing a steam explosion. The high pressure pulse caused by the steam explosion will threaten the integrity of the containment, increasing the risk of the leakage of radioactive substances.

The UK HPR1000 adopts an IVR strategy to avoid fuel-coolant interaction in the reactor pit. IVR can prevent ex-vessel steam explosion by avoiding RPV failure with a high level of confidence according to the demonstration presented in Sub-chapter 13.5.6.3.

If ex-vessel steam explosion occurs, the shock wave produced is usually insufficient to threaten the integrity of the UK HPR1000 containment. Furthermore, the conditions for the occurrence of steam explosion are extremely stringent, with a very low probability of occurrence. The analysis of ex-vessel steam explosion is given in the Level 2 PSA report.

13.5.4.5 Containment Overpressure

Containment overpressure is one possible containment failure mechanism. During severe accidents, containment pressure increase due to the sustained residual heat can occur. If the RPV is intact, the containment pressure increase is mainly due to steam from the evaporation of the RCP [RCS] coolant and IVR injection water. If the RPV fails, the containment pressure increases due to steam and non-condensable gases generated from MCCI.

13.5.4.6 Re-criticality

At the stage of core damage, a problem that may arise from water injection is the possible re-criticality of the core. Core re-criticality can occur because of the difference in temperatures for the failure of control structures versus failure of the fuel. In the time frame that the control rods have melted away while the stack of fuel elements is still largely intact, the injection of water that is not borated or at least

adequately borated may lead to the core re-criticality in the regions of the core without control rods. In principle, the power of the core could increase to the certain amount that evaporates all water injected. Moreover, power peaks are possible if the feedback mechanisms of reactivity addition are not fast enough.

For the UK HPR1000, the re-criticality during in-vessel recovery is unlikely for the following reasons:

- In the early stage of an accident, a large degree of the melting of control rods would not have occurred, therefore, re-criticality will not occur.
- As the accident develops, the control rods may have melted and relocated but the fuel remains in the core, the risk of re-criticality will increase in this stage. However, according to the analysis of severe accident sequences, this stage is very short and the probability of recovering the core cooling in this short interval is significantly small.
- For the UK HPR1000, according to the strategy of injecting water into the primary system, borated water is preferred. In case of severe accidents, the main water source injected into primary circuit comes from IRWST and accumulators, which inject borated water into the core through RIS [SIS]. In addition, the UK HPR1000 has a temporary primary water injection, which can supply water to the primary circuit when RIS [SIS] is not available. The water sources for temporary primary water injection including spent fuel cask loading pit, emergency boric acid tanks and boric acid makeup tank, are borated water sources. If boron injection is conducted, the re-criticality event does not occur.

From the above considerations, it is concluded that the risk of re-criticality during in-vessel recovery is limited for the UK HPR1000.

13.5.5 Descriptions of Severe Accident Mitigation Strategy and Measures

Based on the understanding of severe accident progression and phenomena presented in PCSR Sub-chapter 13.5.3 and 13.5.4, the severe accident phenomena of concern in the UK HPR1000 are identified as shown in T-13.5-5. To maintain the integrity of the barriers between the core and the environment, dedicated severe accident mitigation strategies need to be considered in the design [59][60]. Strategies are designed to cope with the identified phenomena that threaten the integrity of barriers. CGN's experience in previous projects and relevant lessons learnt from Fukushima accident are also the basis of the strategies.

T-13.5-5 SA phenomena and mitigation strategy

SA phenomena	SA mitigation strategy
HPME / DCH	Primary system overpressure protection
Hydrogen combustion	Combustible gas control
Ex-vessel steam explosion /	Corium retention

SA phenomena	SA mitigation strategy
MCCI	
Containment overpressure	Containment heat removal
	Containment filtration and venting

Based on the strategies determined in T-13.5-5, severe accident mitigation systems are designed step by step.

Firstly, safety functional requirements are derived from the strategies. The initial configuration of the systems is based on CGN's experience in previous projects and relevant lessons learned from the Fukushima accident. The evolution process of severe accident mitigation measures in CGN is introduced in the report "*ALARP Demonstration Report for Severe Accident Analysis"* [59].

Secondly, severe accident analysis is performed based on the preliminary design to determine the size and layout of equipment and time allowance for operator actions. Iterative design among different technical areas may be needed to solidify the detailed design. During this process, requirements on categorisation & classification, equipment qualification, I&C, electrical engineering, structural integrity, human factors (operator action and human accessibility), and civil engineering are considered.

The mitigation measures include:

a) Severe Accident Dedicated Valve (SADV) to prevent containment over-heating and overpressure caused by high-pressure melt ejection.

b) EUH [CCGCS] to reduce hydrogen concentrations and risk from combustion and explosion.

c) EHR [CHRS] to prevent containment overpressure failure by spraying.

d) IVR strategy is achieved by reactor pit flooding system, which is the sub-system of EHR [CHRS]. The system diagram of EHR [CHRS] is shown in Sub-chapter 7.4.2. Reactor pit flooding system is designed to maintain the corium within the RPV, thus preventing ex-vessel steam explosion, MCCI, DCH and maintaining the integrity of the containment.

e) EUF [CFES] is the ultimate way to prevent containment overpressure and limit the release of radioactivity within acceptable levels.

Detailed descriptions of these measures can be found in chapter 6 and chapter 7. As suppliers of the severe accident management equipment will not be determined in the GDA process of the UK HPR1000, the qualification specifications of equipment will instead be provided. The qualification specifications for each system will be based on the output of the SAA to ensure that the systems will be able to perform as intended

and deliver their safety function under the conditions they will be required to operate.

13.5.5.1 SADV

13.5.5.1.1 Safety Functions

Failure of the RPV under high internal pressure is of great importance to severe accident risk as missiles could be created from vessel movement. HPME could lead to DCH by melt debris dispersing inside the containment atmosphere, which could result in subsequent containment failure. Therefore, the ability to reduce the pressure of primary system under severe accidents should be ensured so that HPME can be avoided. In the UK HPR1000, the dedicated SADVs are specially designed for primary system depressurisation under severe accidents and achieve the following safety functions:

a) To be opened when required and remain opened that allowing sufficient flow rate to depressurise the primary circuit.

b) To avoid the high pressure core melt situations and subsequent HPME and DCH by depressurising the primary pressure during severe accident conditions, which can restrict the release of radioactive substances.

c) To prevent the induced creep rupture of SG tubes and subsequent containment radiological bypass by reducing the natural circulation of hot gases through the primary circuit.

Even in the case of loss of offsite power and failure of all emergency diesel generators, the SADVs are able to be opened when required and remain opened, or they are able to remain closed – no leak or fail – until they are opened by the operator.

13.5.5.1.2 Design Basis

In case of a severe accident occurring in the reactor, the SADVs are opened manually under a certain condition (e.g. when the core outlet temperature reaches 650°C) to ensure the pressure of the RCP [RCS] to be lower than 2.0 MPa abs. before RPV failure [61], thus avoiding the high-pressure core melt accident.

13.5.5.1.3 Design Process

In UK HPR1000, the SADV is designed with a systematic method including the following steps:

a) Step 1: Design object is determined by depressurising the primary system under severe accident conditions to avoid high-pressure core melt accident.

b) Step 2: Functional requirement is determined by ensuring the pressure of the RCP [RCS] is lower than 2.0 MPa abs. before RPV failure by depressurising under a certain condition (e.g. when the core outlet temperature reaches 650°C).

c) Step 3: The sizing conditions are determined by considering sequences with high primary pressure according to the deterministic and engineering judgement.

d) Step 4: Sizing of SADV is determined by the following steps shown in Figure F-13.5-3:

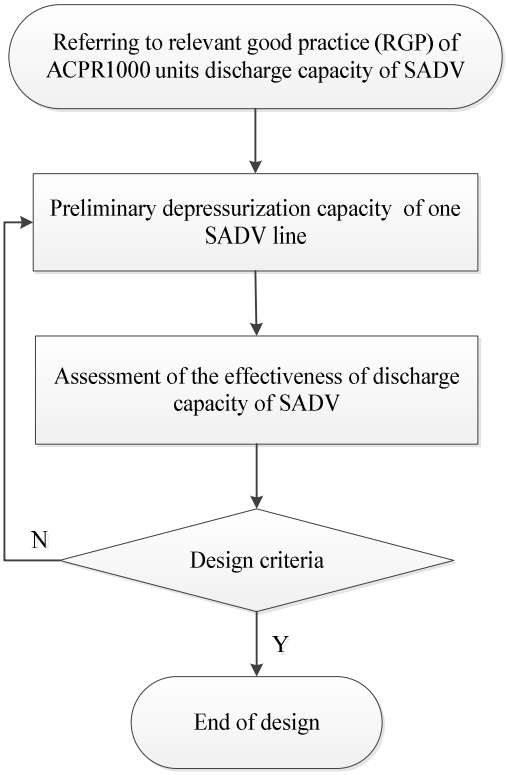
1) Referring to RGP for ACPR1000 units, the discharge capacity of one SADV line is equal to the total discharge capacity of the three PSVs.

2) Considering the discharge capacity of one PSV is 210 t/h for the UK HPR1000, the preliminary discharge capacity of one SADV line of UK HPR1000 is determined to be 630 t/h (3×210 t/h).

3) Assessing the effectiveness of the preliminary discharge capacity of SADV under the design criteria, which means to depressurise the RCP [RCS] pressure lower than 2.0 MPa abs. before RPV failure.

4) According to the assessment result, the discharge capacity of the SADV is to be adjusted and the above assessments conducted again until the design criteria are met.

e) Step 5: A last round of analysis and assessment is performed to prove the effectiveness of the SADV discharge capability. The assessment process ensures that the SADV design meets the requirements of primary depressurisation.



F-13.5-3 The Design Flow Chart of SADV Depressurisation Capacity

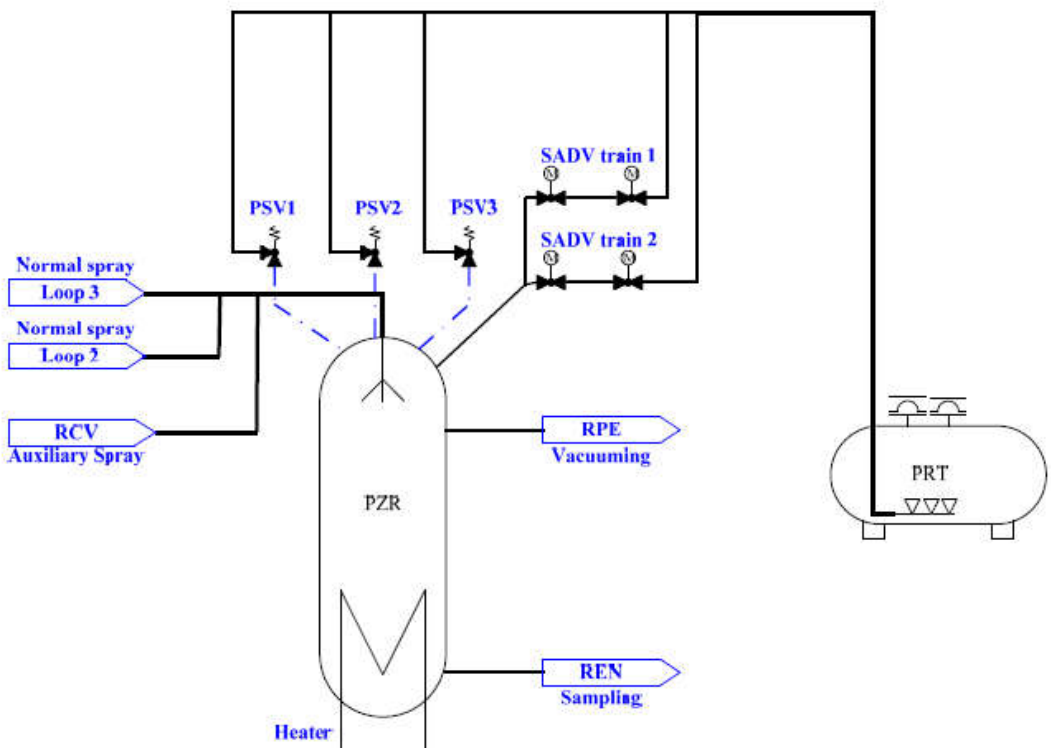
13.5.5.1.4 Mitigation Measures

The ability to reduce the primary system pressure under severe accidents with high pressure is achieved by the SADVs on the two discharge lines on top of the pressuriser. Each line includes two motorised valves in series that are connected to the same pressuriser nozzle, which is located at the same elevation as the nozzles of the PSVs. One of the two motorised valves in series in each line ensures the isolation function. Both the SADVs and PSVs are connected to the pressuriser relief tank though lines.

The depressurisation capacity of the SADVs in UK HPR1000 is designed as follows:

The required discharge capacity of one SADV line has been established to be 630t/h at 17.23MPa abs. in saturated steam conditions.

The functional diagram of the SADV is shown in Figure F-13.5-4 and the detailed information of the SADV is described in Reference [62].



F-13.5-4 The Functional Diagram of the SADV

During the design process of the SADV, requirements on categorisation & classification, equipment qualification, electrical engineering, I&C, plant autonomy , human factors (operator action and human accessibility), and civil engineering are considered as follows

a) Categorisation & classification

The SADVs are classified following the general principles of safety classification in the UK HPR1000 [63]. Both SADVs and the discharge lines downstream of SADVs are classified as FC1 level [62].

b) Equipment qualification

The components of the SADVs that are required to perform safety functions are environmental qualified to ensure the functionality. The detailed information refers to Reference [62].

c) Electrical engineering

The SADVs are equipped with EDGs, SBO diesel generator and 24-hour batteries. In the event of total loss of alternating current power, the SADVs are equipped with mobile power supply devices.

d) I&C

To realise the safety functions, I&C functional requirements of the SADVs are considered. Normally, the I&C functions associated with the SADV are controlled automatically or manually in the main control room. Detailed information can be found in Reference [64].

e) Operator action

The SADVs are designed to be opened by the operator in the main control room. In order to improve the function reliability, the human factor requirements of SADVs are considered. Detailed information can be found in Reference [62].

13.5.5.2 EUH [CCGCS]

Under severe accidents, hydrogen can be generated and released to the containment. The mixture of hydrogen and atmospheric air may burn when the hydrogen concentration exceeds 4 vol%. When the hydrogen concentration exceeds 10 vol% [65], flame acceleration up to sound velocity has been found in many experiments and, in extreme cases, flame may accelerate to detonation conditions, a phenomenon known as DDT. Flame acceleration and DDT can be destructive and potentially threaten the containment integrity. In order to prevent containment failure due to hydrogen combustion in the containment, the EUH [CCGCS], which consists of Passive Automatic Recombiners (PARs) sub-system and hydrogen monitoring sub-system, is designed for the UK HPR1000.

13.5.5.2.1 Safety Functions

The safety requirements of reactivity control and residual heat removal are not required by the EUH [CCGCS] system. The main safety function of the EUH [CCGCS] is to maintain the integrity of the containment and thus limit the radioactive materials in the containment.

To be more practical, main safety functions of the EUH [CCGCS] are detailed as follows:

a) Limiting and reducing local hydrogen accumulation within the containment.

b) Limiting the average hydrogen concentration in the containment to be below 10 vol % under severe accidents.

c) Eliminating the risk of containment failure caused by hydrogen combustion during severe accidents.

d) Indicating the hydrogen concentration in the containment to operators in MCR.

13.5.5.2.2 Design Basis

The design basis of the EUH [CCGCS] for the UK HPR1000 is set as follows:

a) Hydrogen concentration in the containment must be limited to be less than 10 vol% supposing that hydrogen is uniformly distributed.

b) If local flame acceleration occurs, the integrity of the containment must be maintained.

13.5.5.2.3 Design Process

The EUH [CCGCS] is designed to eliminate the hydrogen and thus reduce the containment failure risk due to hydrogen combustion. The design process includes many steps including the determination of the hydrogen control requirements, determination of the number of PARs and determination of layout for the PARs.

a) The first step is to determine the design objective of the system, which is to eliminate the hydrogen and thus mitigate containment failure risk due to hydrogen combustion.

b) The second step is to develop the design basis.

c) The third step is the design process of EUH [CCGCS]. This includes the preliminary decision of the number of the PARs and their layout, considering the hydrogen control requirement, the hydrogen production rate, system margins and the layout of the containment. Determination of the layout of PARs is made firstly by considering the possible sources of hydrogen and the hydrogen concentration in each compartment. The design is iterated with the availability of the localisation based on the containment layout and other relevant aspects.

d) The fourth step is the analysis and assessment of the effectiveness of the EUH [CCGCS], which ensures that the EUH [CCGCS] design meets the hydrogen control requirement after design iterations.

In the determination of the number of PARs for the UK HPR1000, good practice from CPR1000 is applied in the preliminary design. Then, margins are considered to cover

the uncertainties on the recombination of PARs and the availability of localisation is assessed. Iterative analysis is performed to finalise the number of PARs. In the UK HPR1000, 29 PARs including 11 small-size PARs and 19 large-size PARs are equipped in the containment to reduce the local and global hydrogen concentrations.

In the process of determining the layout of the PARs, the layout principles aiming to reduce hydrogen risk ALARP are applied. These principles are shown as follows:

1) Locate the PARs in the middle and upper level in the containment to optimise the natural convection.

2) Locate the PARs in the compartments where the hydrogen risk is relatively high to avoid the local build-up of hydrogen.

3) Locate the PARs in the compartments that the hydrogen may release into directly.

4) Avoid damage of other important equipment considering the layout of the containment.

5) Locate PARs in locations that are easy to access, thus keeping the PARs in good condition.

13.5.5.2.4 Mitigation Measures

The EUH [CCGCS] consisting of a PARs sub-system and a hydrogen monitoring sub-system designed to mitigate the hydrogen risk. The PARs consist of several catalyst plates at their inlets, where hydrogen reacts under the principle of catalytic chemistry. By this principle, the PARs are capable of working when hydrogen concentration reaches the threshold value (2 vol%). In fact, the EUH [CCGCS] can reduce the hydrogen concentration in the containment in both severe accidents and DBC such as LOCA. The EUH [CCGCS] is not running under normal operation conditions, and it can start up automatically without manual operation following the design basis accidents and severe accidents.

A total number of 29 PARs are equipped in the containment in locations that facilitate natural convection. Among the 29 sets of PARs in the UK HPR1000, 27 sets of PARs are set to recombine the hydrogen under severe accident conditions. For these PARs, the function class is F-SC3 and equipment qualification is required under severe accident environmental conditions. Another 2 PARs are designed with the same equipment qualification requirement as that for the 27 PARs combined with a higher level function class of F-SC2, because these 2 sets of PARs that are designed for both DBC conditions and severe accident conditions. Therefore, all the 29 sets of PARs are capable of managing hydrogen risk during severe accident conditions. The present report credits all the 29 sets of PARs.

In addition, the hydrogen monitoring system is designed to indicate the hydrogen risk and assist the manual operation during SAMG. The hydrogen monitoring system

contains two redundant trains, each fitted with local hydrogen sensors. Each train consists of five hydrogen sensors installed in the containment dome, annulus space and top of the SG compartments.

The hydrogen monitoring sub-system is powered by offsite power at normal condition. When LOOP occurs, SBO diesel generators and the emergency diesel generators are used as the backup power. When all the diesel generators are unavailable, batteries are used to supply power.

The operator can start or stop the hydrogen monitoring sub-system in the main control room. The hydrogen monitoring system is manually operated in the case of accidents. The containment hydrogen concentration signal detected online by the hydrogen monitoring subsystem will be displayed in the main control room and remote shutdown station.

13.5.5.3 IVR

13.5.5.3.1 Safety Functions

During a severe accident, the core may melt due to insufficient cooling. The corium will relocate to the lower head of the RPV. Since the temperature of the corium is much higher than the melting point of the RPV, the RPV will be melted through and a number of severe accident phenomena such as steam explosion and MCCI may occur if no mitigation measures are applied.

The IVR strategy has been implemented in the UK HPR1000 to maintain the integrity of the RPV. Not only can cooling water be passively injected into the reactor pit from the IVR water tank, but also the water of the IRWST can be actively injected into the reactor pit to cool the outside of the RPV and remove heat from the corium pool. Therefore the IVR strategy can prevent RPV failure, thus avoiding many ex-vessel phenomena (DCH, steam explosion and MCCI) which may threaten the containment integrity.

13.5.5.3.2 Design Basis

In order to retain the corium inside the RPV after severe accidents, the following two success criteria need to be met:

a) The heat flux transferred from the corium to the outer surface of RPV lower head must be lower than the local Critical Heat Flux (CHF), namely the RPV wall cannot be melted through in steady state.

b) When part of the RPV lower head wall has been ablated by molten corium, the minimum thickness still has enough mechanical strength to maintain the RPV integrity.

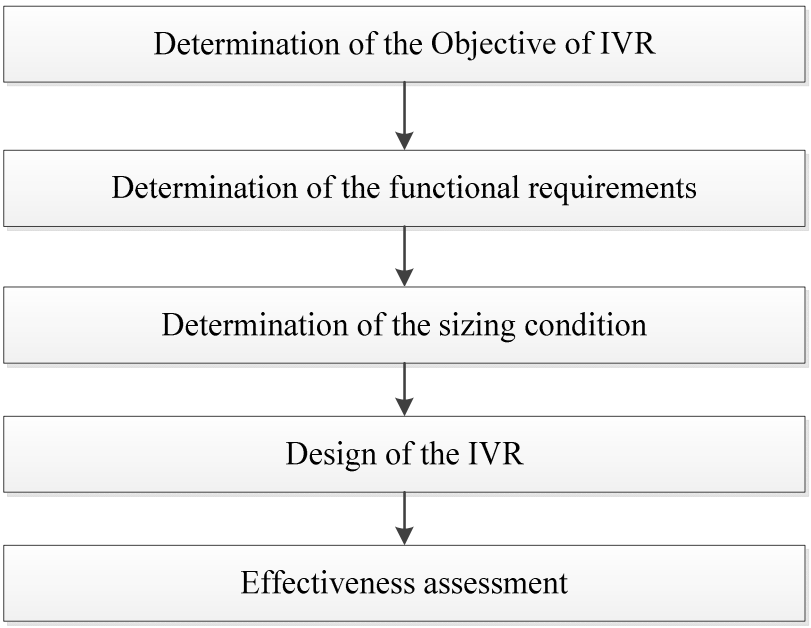
The IVR strategy is one of the important severe accident mitigation measures for the UK HPR1000. It has no safety-related functional requirements under normal

operation conditions, shutdown and refuelling conditions. Furthermore, it is important to ensure that the injection systems are not activated under normal operation conditions and shutdown conditions. It is required that the electricity supply to relevant valves will be established once the core outlet temperature reaches 650°C.

The water injection pipeline, water level monitoring instrumentation, temperature monitoring instrumentation and other components in the reactor pit should consider the gas density and not affect the operation of the reactor pit ventilation system under normal conditions.

13.5.5.3.3 Design Process

The flow chart of IVR design process is shown in F-13.5-5. Firstly, the objective of the IVR and functional requirements is determined. Secondly, the preliminary design of the IVR system is carried out based on the results of the sizing condition analysis and structure arrangement of reactor pit. Finally, a series of calculation and tests are performed to verify the effectiveness of the IVR.



F-13.5-5 The flowchart of IVR design process

The objectives of IVR are listed as follows.

1) Cool the core debris and keep the integrity of RPV.

2) Restrict releases of radioactive substances.

For the functional requirements, the reactor pit should be flooded passively in a short time. The water level of the reactor pit should remain at a high value, taking into account vaporization of some of the water inventory. The RPV should be cooled sustainably by natural circulation without the use of AC electricity. When the AC electricity recovers, the passive water injection is switched to active water injection

for long term operation.

According to the severe accident progression, the larger break of the primary loop, the larger flow rate of the coolant loss. In addition, more decay heat exists in the corium pool. Therefore, the IVR strategy is required to be activated earlier and a larger flooding flow rate is needed. So the initial condition of LB-LOCA is employed as a sizing condition.

Based on the functional requirements and the severe accident progression of the sizing condition, the design of the IVR is determined. Both passive water injection and the active water injection are employed to ensure the reactor pit to be flooded.

The natural circulation cooling of the RPV is significant after severe accident, especially under the SBO condition. So a reliable natural circulation flow channel is designed. The natural circulation flow channel consists of the recirculation loops, reactor pit and annular passage between the Reflective Metallic Insulations (RMI) and the outside surface of RPV.

Based on the core melt process of the sizing condition, the reactor pit should be flooded approximately 30 minutes after the activation of the reactor pit flooding system.

During the design process, requirements on categorisation & classification, equipment qualification and I&C have been considered to make sure the values and measuring instruments are available under severe accident conditions.

For operation, according to the results of bounding case, the reactor pit flooding system should be actuated 20 minutes after entering SAMG. The precondition for the activation of reactor pit flooding system is the successful primary depressurisation which needs the operator to open the dedicated SADVs manually. When the water level of IVR tank is lower than 1.14 m, the alarm for low water level is actuated and the operator can start the EHR [CHRS] pump to inject water into the reactor pit in approximately 30 minutes.

For electrical engineering, the reactor pit flooding system, which is a sub-system of the EHR [CHRS], can be powered by an electrical division and backed-up by the EDG. This sub-system is powered by SBO diesel generators when the EDG fails. It is also supplied by mobile diesel generators to ensure its function under extreme accidents such as Fukushima accidents. The isolation valves of the passive flooding are also powered by 24 h battery.

For the effectiveness assessment, both thermal analysis and mechanical analysis are taken into account to assess the effectiveness of the IVR.

13.5.5.3.4 Mitigation Measures

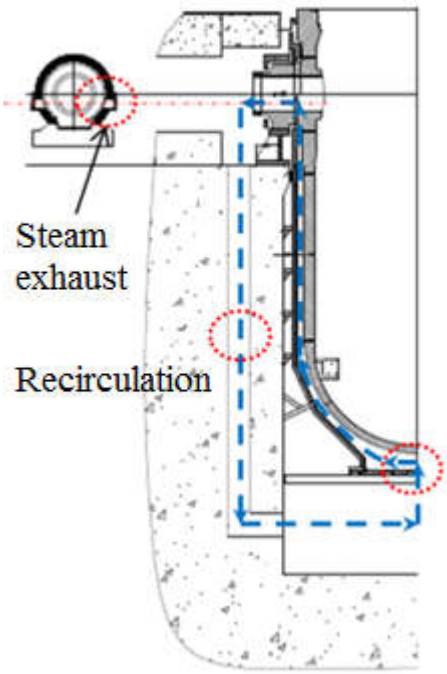
The reactor pit flooding system consists of two injection pipelines: the passive

injection pipelines and active injection pipelines. The passive IVR lines inject water from the IVR tank while active IVR injects water from the IRWST.

When the core outlet temperature reaches 650ºC, operators manually open the passive injection line isolation valves within 20 minutes. The isolation valves can be powered by the Uninterruptible Power Supply (UPS) batteries to guarantee its availability even if the SBO diesel generators & EDGs fail. Passive injection does not need AC power. The passive injection consists of two phases: the large flow rate phase to flood the cavity within half an hour and the small flow rate phase to compensate for the water evaporation. The valve opening time and flow rate have been justified by the bounding severe accidents sequence (LB-LOCA).

There is no need to close the isolation valves. When the IVR tank is empty, water will be pumped into the cavity from the IRWST. The motor-operated valves of the reactor pit flooding system are located in different compartments on the SADV discharge line. The opening of the SADV has little impact on the reliability of the reactor pit flooding system valves.

To ensure the effectiveness of the IVR strategy, an RPV insulation layer is designed. Inlets for the water and outlets for steam are designed. After water is injected into reactor pit under severe accident conditions, the water inlets and steam outlets can be opened passively to provide a smooth flow channel for natural circulation. The design of the flow channel is optimised based on relevant tests and analysis.



F-13.5-6 Sketch design of flow channel

13.5.5.4 EHR [CHRS]

13.5.5.4.1 Safety Functions

Due to steam accumulation in severe accidents, containment pressure increases slowly and continuously without mitigation measures. Finally, containment pressure reaches the containment design pressure, thus leading to risk of containment failure in the long term. In the UK HPR1000, the EHR [CHRS] is designed for long-term containment heat removal and containment pressure control under severe accidents.

It should be noted that the EHR [CHRS] consists of passive reactor pit water injection, active reactor pit water injection and a containment spray sub-system. This report focuses on the spray mode of the EHR [CHRS] which implements the function of the containment heat removal under severe accidents. In the following context the EHR [CHRS] refers to the containment spray sub-system. The details of the IVR strategy, including passive reactor pit water injection and active reactor pit water injection, are introduced in Sub-chapter 13.5.5.3.

The safety functions of the EHR [CHRS] are listed as follows:

a) Transfer the residual heat of the containment atmosphere to the IRWST in order to control the containment pressure under severe accidents.

b) Transfer the heat of the IRWST to the UHS.

c) Reduce the aerosol concentration in the containment atmosphere.

d) Ensure the containment integrity.

The containment system of the UK HPR1000 can provide a 12-hour operator non-intervention grace period after severe accidents. During this time, the pressure in the containment can be kept lower than the design pressure without any operator action [41]. After the 12-hour grace period, the actuation of the EHR [CHRS] is required to remove the containment heat to avoid containment overpressure failure and ensure finally the confinement of radioactive substances in the containment.

13.5.5.4.2 Design Basis

To realise the safety functions, the following design basis need to be met:

a) Short-term function criteria:

    1) Activating two trains of the EHR [CHRS] after the 12 hours' grace period allows reduction of the pressure of the containment below { } within 24 hours after system operation.

    2) Activating one train of the EHR [CHRS] after the 12 hours' grace period enables the pressure of the containment to be maintained below the design pressure (0.52 MPa abs).

b) Long-term function criteria:

During the long-term operation of the EHR [CHRS], one train of the EHR [CHRS] ensures that the pressure of the containment is maintained below { }.

13.5.5.4.3 Design Process

In the UK HPR1000, the EHR [CHRS] is designed with a systematic method including the following steps:

1) Step 1: Design object is determined considering containment heat removal to avoid containment overpressure failure and the confinement of radioactive substances.

2) Step 2: Functional requirements are determined considering heat removal from containment and confinement of radioactive substances.

3) Step 3: The sizing conditions are determined considering the most enveloping conditions with the most mass and energy released into the containment.

4) Step 4: Sizing of the main equipment of EHR [CHRS] depends on engineering justification and calculations, from which a set of preliminary design values are determined. Then the design is iterated with the system effectiveness assessment taking into account different design aspects. Finally the design values are consolidated, which include the heat load per train, cold side flowrate and the hot side flowrate.

5) Step 5: A last round of analysis and assessment is performed to prove the effectiveness of the EHR [CHRS]. The assessment process ensures that the EHR [CHRS] design meets the containment pressure control requirement.

13.5.5.4.4 Mitigation Measures

The containment spray sub-system has two identical trains isolated physically.

Each train mainly includes:

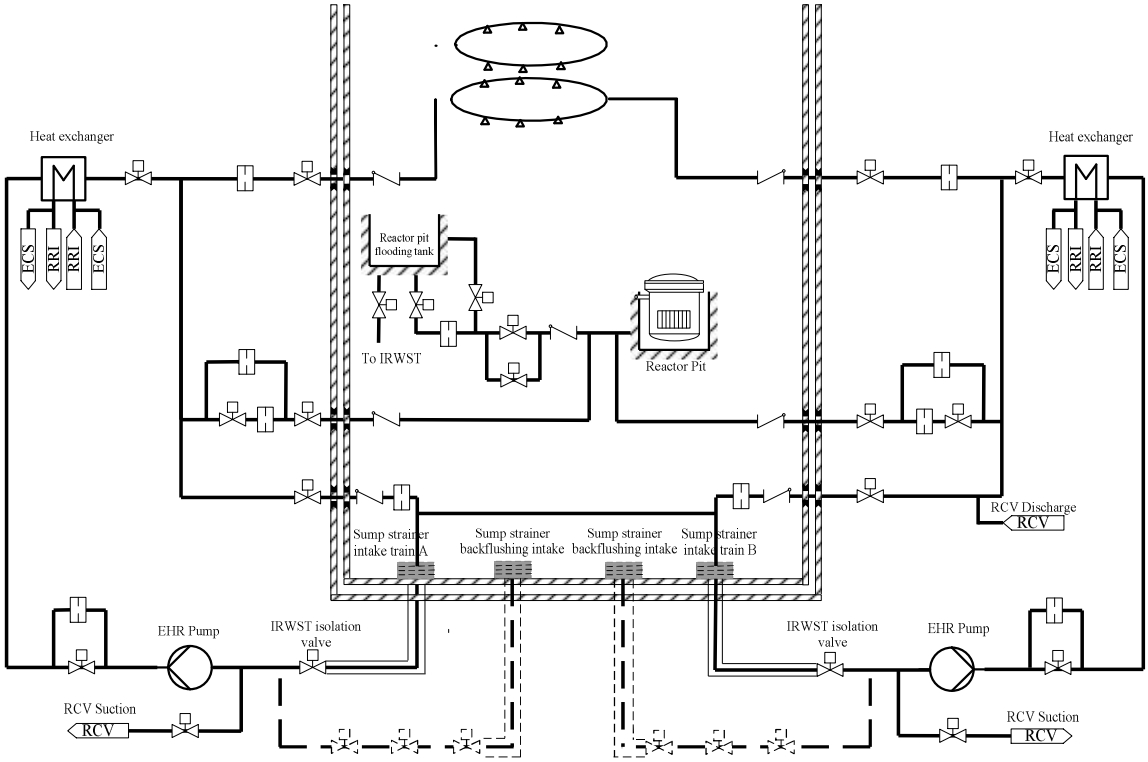
a) An intake line from the IRWST.

b) One pump.

c) One heat exchanger.

d) One discharge line (for spray).

The functional diagram of the EHR [CHRS] is shown in F-13.5-7. The detailed information of EHR [CHRS] is described in Reference [66] and [67].



F-13.5-7 The Functional Diagram of the EHR [CHRS]

During the design process of the EHR [CHRS], requirements on categorisation & classification, equipment qualification, electrical engineering, I&C, plant autonomy, operator actions, and interfaces to other systems are considered.

1) Categorisation & classification

The EHR [CHRS] is classified following the general principles of safety classification in the UK HPR1000 [63]. The containment isolation is classified as FC1, and other system function of the EHR [CHRS] are classified as FC3 [67].

2) Equipment qualification

The components of EHR [CHRS] which are required to perform safety functions are environmentally qualified to ensure the functionality. Detailed information can be found in References [67] [68].

3) Electrical engineering

The EHR [CHRS] is required to perform safety functions under DEC. In order to improve the function reliability, the electrical equipment of two trains is powered by separate electrical partitions. The main equipment of the EHR [CHRS] (including pump motor, electric valves, etc.) is equipped with EDG, SBO diesel generator and mobile power supply devices besides the normal off-site power supply. The electrical equipment for total loss of AC power conditions is equipped with 24-hour battery, such as the containment isolation valves, reactor pit flooding isolation valves, etc. [69]

4) I&C

To realise the safety functions, I&C functional requirements of EHR [CHRS] are considered. Normally, the I&C functions associated with the EHR [CHRS] are controlled automatically or manually in the main control room. The detailed information can be found in Reference [70].

5) Grace period and plant autonomy

According to the reference [41], the requirements of autonomy of EHR [CHRS] are considered, which includes autonomy in respect of operators, autonomy in respect of heat sink and autonomy in respect of power supply systems.

6) Operator actions

The EHR [CHRS] start-up is designed to be manually started by the operator in the main control room. In order to promote the success of operator actions, the time available for action, the conditions to be expected and the psychological demands being made on the operator are considered. Detailed information can be found in reference [67].

7) Interfaces to other systems

During the design of the EHR [CHRS], the performance of the interface systems are considered. The interface systems mainly consist of supporting systems and user systems. Detailed information can be found in reference [69].

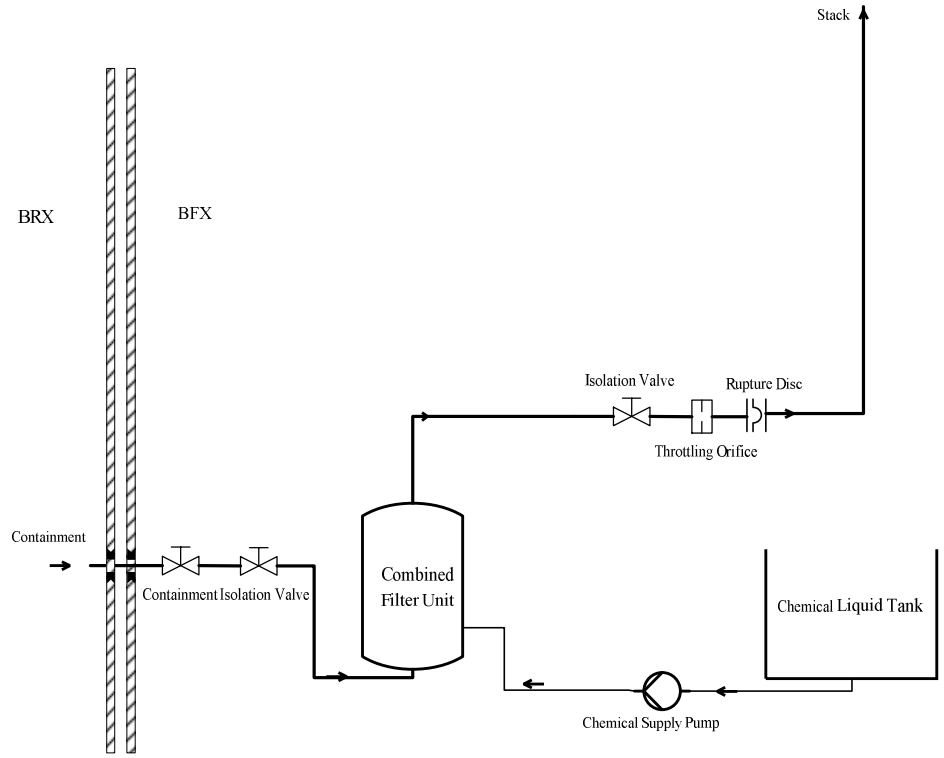
13.5.5.5 EUF [CFES]

The design of the EUF [CFES] is based on the HPR1000 (FCG3) and may change for the UK HPR1000 according to further research.

13.5.5.5.1 Safety Functions

According to the nuclear safety design concept of defence in depth, containment spray of the EHR [CHRS] is the primary measure to control containment pressure during severe accidents. The EUF [CEFS] is an alternative way to mitigate the risk of containment overpressure when the containment spray of EHR [CHRS] is unavailable.

The EUF [CFES] controls containment pressure by venting and filtering containment atmosphere to the environment. The decontamination factors of aerosol, element iodine and organic iodine are 1000, 100 and 5, respectively.



F-13.5-8 Schematic Diagram of the EUF [CFES]

13.5.5.5.2 Design Basis

In the design of EUF [CFES], the following design basis conditions need to be met:

1) The depressurisation capability of EUF [CFES] should continuously decrease the containment pressure.

2) The depressurisation and operation capability of EUF [CFES] should allow a period of time for the replenishment of water and chemical drugs of EUF [CFES].

13.5.5.5.3 Design Process

In the UK HPR1000, the EUF [CFES] is designed with a systematic method including the following steps:

1) The design objective of EUF [CFES] is determined considering the containment depressurisation.

2) The functional requirements are defined considering containment depressurisation and radioactive substance release from containment.

3) According to the design objective, identify the most challenging scenarios similar to the Fukushima accident to EUF [CFES].

4) Perform transient analysis with severe accidents analysis code to get the containment response of these challenging scenarios.

The last round of analysis and assessment is performed to prove the effectiveness of EUF [CFES]. The assessment process ensures that EUF [CFES] design meets the containment depressurisation control requirement.

13.5.5.5.4 Mitigation Measures

24 hours after the accident occurs and when containment pressure is over the design pressure (0.52 MPa abs.), the EUF [CFES] can be operated. However, the approval to open the EUF [CFES] is decided by the emergency organisation.

The EUF [CFES] reduces containment pressure by venting and filtering containment atmosphere. The mixture gases, which are released to the environment, flow through the inlet line and containment isolation valves, then go through combined filter unit, restriction orifice and rupture disk in turn, finally reaching the chimney.

When the containment pressure is 0.52 MPa abs., the venting mass flow is approximately 4kg/s. The system should not be clogged by aerosol. By manually local opening or closing the isolation valves, operators can activate or stop the operation of the EUF [CFES]. The water and chemicals of the combined filter unit can support the operation of the EUF [CFES] with the designed filter efficiency. If containment spray of the EHR [CHRS] recovers at any time, the operation of the EUF [CFES] should be terminated.

The schematic diagram of EUF [CFES] is shown in F-13.5-8. The main components of the EUF [CFES] are listed as follows [71] [72]:

1) Containment isolation valve

Two containment isolation valves are installed in the inlet line of the EUF [CFES] for containment isolation. The isolation valves can be driven manually behind the shield wall through a remote transmission mechanism.

2) Combined filter unit

The radioactive substances released from the containment atmosphere are filtered by the combined filter unit. The filtered substances are mainly aerosols and iodine. The chemical liquid tank can continue to supply the combined filter unit for 12 hours without operator intervention.

3) Restriction orifice

One restriction orifice set is installed in the outlet line of the combined filter unit to restrict the discharged gas flow of the EUF [CFES], so that the combined filter unit can operate at a relatively broad pressure range and maintain the best filtration performance.

4) Rupture disk

Rupture disk is located behind the restriction orifice. The protection function with

nitrogen filling is maintained under the standby mode of the EUF [CFES]. After the EUF [CFES] operates, the system pressure reaches the set point value of the rupture disk, which will open and the filtered gases will discharge to the environment.

During the design process, requirements on categorisation & classification, equipment qualification, I&C, electrical engineering, structure integrity and human factors (operator action and human accessibility) have been considered.

1) Categorisation & classification

The containment isolation is classified as Function Category 1 (FC-1). The filtration and exhaust are classified as Function Category 3 (FC-3) [68].

2) Equipment qualification

The equipment to be qualified is categorised into several qualification categories based on its location and the conditions under which they perform the intended functions. See the reference [71] for details.

3) I&C

The EUF [CFES] is started by the manual opening of the containment isolation valves.

4) Human factors

After 24 hours following severe accidents, when the pressure of containment is higher than its design pressure (0.52MPa abs.), the EUF [CFES] is started by manually opening the containment isolation valves.

The layout of the EUF [CFES] ensures that the containment isolation valves to be operated are accessible for the personnel. Furthermore, radiation protection walls are arranged to protect the personnel [73].

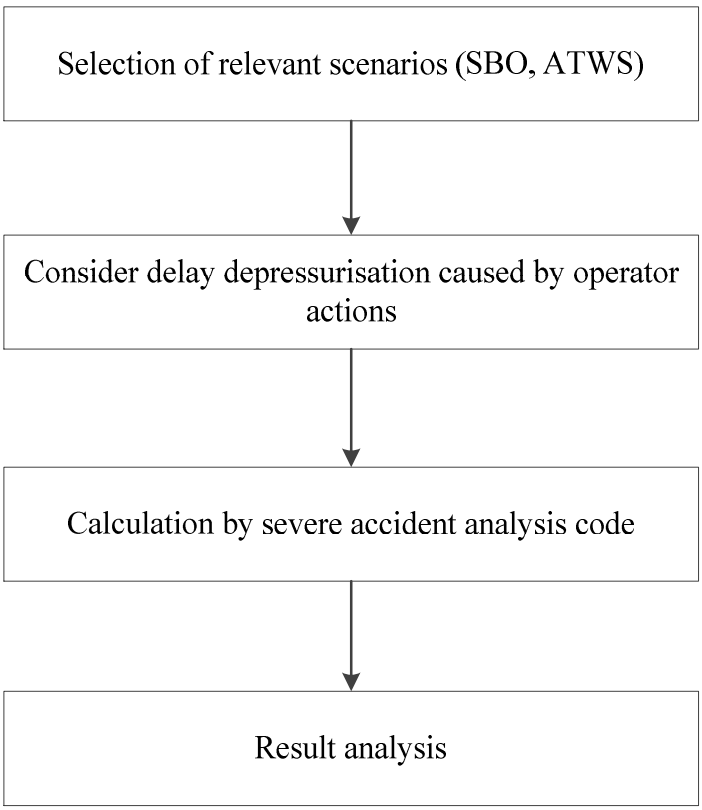
13.5.6 Assessment of SA Mitigation Measures

Based on the selection process in Sub-chapter 13.5.2, the DEC-B sequences listed in Table T-13.5-4 are analysed based on best estimate assumptions to demonstrate the effectiveness of the mitigation measures.

13.5.6.1 Assessment of SADV

13.5.6.1.1 Methods for the Assessment of SADV

The analysis to justify the effectiveness of the SADVs discharge capability of the UK HPR1000 is performed based on the capacity of the SADVs with a mass flow rate of 630 t/h. Several steps are taken to assess the SADVs. The effectiveness analysis flow chart is listed as follows:



F-13.5-9 The Flow Chart of SADV Effectiveness Analysis

a) Selection of relevant scenarios

The objective of SADV design is to transform high pressure core melt scenarios to low pressure core melt scenarios with high reliability, so that high pressure core melt situations can be prevented. To assess the effectiveness of SADV, it is reasonable to select the sequences with high primary pressure to verify whether the discharge capability of SADV is sufficient for primary depressurisation. According to the deterministic assessment and engineering judgement, ATWS and SBO are selected to be analysed.

b) Consideration of delay depressurisation caused by operator actions

RCP [RCS] depressurisation by SADV is a manual action. Considering the time gap between the triggering of SADV open signal and the depressurisation activated by the operator actions, the delay depressurisation caused by operator actions should also be taken into account. A delay time of 30 minutes to RCP [RCS] depressurisation is assumed in the following analysis, which provides a significant time margin for the operator actions.

c) Calculation by severe accident analysis code

Calculations are performed by using ASTEC code, the description of which is given in Appendix 13A. The accident assumptions are shown in Sub-chapter a).

d) Result analysis

Effectiveness of the assessment of the SADV is based on the calculation results. The detailed analysis results refer to Reference [74].

13.5.6.1.2 Event Description

As described above, SBO and ATWS sequences are chosen to demonstrate the efficiency of the discharge capability of the SADV to transform high pressure core melt scenarios to low pressure ones, and delayed depressurisation should also be analysed. The detailed descriptions are as follows.

13.5.6.1.2.1 SBO

After SBO, the decay heat cannot be timely removed from the core if secondary cooling fails, which leads to an increase of primary pressure. The PSVs open automatically when primary pressure increases to the threshold value, which results in a loss of primary coolant. Subsequently, the core uncovers. When the core outlet temperature reaches 650°C, the SADVs are opened by operator action in the main control room for primary depressurisation.

The initial conditions for the accident analysis are as follows:

a) The reactor initially operates at full power condition.

b) The sequence is initiated by LOOP with the loss of the emergency diesel generators.

The related assumptions for accident analysis are as follows:

a) SBO diesel generators unavailable.

b) ASG [EFWS] unavailable.

c) ASP [SPHRS] unavailable.

d) RIS [SIS] accumulator available.

e) MHSI unavailable.

f) LHSI unavailable.

g) Containment spray of EHR [CHRS] unavailable.

h) IVR is not considered.

i) The PSVs are closed when the SADVs are opened for conservative consideration.

To verify the depressurisation capacity of the SADV, three different opening conditions of SADVs are considered as follows:

- Case 1, assuming no SADVs can be used, only PSVs can open automatically to

depressurise primary pressure when it increases to the threshold value.

- Case 2, when the core outlet temperature reaches 650°C, the SADVs are opened manually without delay.
- Case 3, when the core outlet temperature reaches 650°C, it is considered that the SADVs are opened after a 30 min delay.

13.5.6.1.2.2 ATWS

After the loss of the main feedwater, the reactor trip fails and the ASG [EFWS] is unavailable, which leads to a decrease of the capacity to remove decay heat by the secondary circuit. Primary temperature and pressure rise. The PSVs open automatically when the primary pressure increases to the threshold value, resulting in a loss of primary coolant. Subsequently, the core uncovers. When the core outlet temperature reaches 650°C, the SADVs are opened by operator action in the main control room for primary depressurisation.

The initial conditions for the accident analysis are listed as follows:

a) The reactor is initially operated at full power conditions.

b) The sequence is initiated by loss of the main feedwater and reactor trip fails.

The related assumptions for the accident analysis are listed as follows:

a) ASG [EFWS] unavailable.

b) RIS [SIS] accumulator available.

c) MHSI unavailable.

d) LHSI unavailable.

e) Containment spray of EHR [CHRS] unavailable.

f) IVR is not considered.

g) The PSVs are closed when the SADVs are opened for conservative consideration.

To verify the depressurisation capacity of the dedicated severe accident depressurisation valves, three different starting conditions of the valves are considered as follows:

- Case 4, assuming no SADV can be used, only PSVs can open automatically to depressurise primary pressure when it increases to the threshold value.
- Case 5, when the core outlet temperature reaches 650°C, the SADVs are opened manually without delay.
- Case 6, when the core outlet temperature reaches 650°C, it is considered that the SADVs are opened after a 30 min delay.

13.5.6.1.3 Effectiveness Evaluation of SADV

In this section, six cases are calculated with ASTEC code to evaluate the effectiveness of the SADV. The description of the code is given in Appendix 13A.

13.5.6.1.3.1 SBO

a) Case 1

For this scenario, assuming no SADVs can be used, only the PSVs can be used to depressurise the primary pressure by opening automatically when primary pressure increases to its threshold value.

According to the analysis results, the primary pressure is 15.6 MPa abs. at the moment of RPV failure, which is far more than 2.0 MPa abs. This analysis reveals that the primary pressure cannot be depressurised to lower than 2.0 MPa abs. before RPV failure if only PSVs open automatically when primary pressure increases to the threshold value. The detailed analysis results can be found in Reference [74].

b) Case 2

For this scenario, the SADVs are opened when core outlet temperature exceeds 650 °C, and the primary pressure drops quickly after the SADV are opened.

According to the analysis results, the primary pressure is 0.35 MPa abs. at the moment of RPV failure, which is far less than 2.0 MPa abs. There is a significant margin between the RCP [RCS] pressure when RPV failure and 2.0 MPa abs. The detailed analysis results can be found in Reference [74].

c) Case 3

For this scenario, the opening time of SADVs is delayed by 30 minutes after the core outlet temperature reaches 650°C, and the primary pressure drops quickly after the SADV are opened.

According to the analysis results, the primary pressure is 0.27 MPa abs. at the moment of RPV failure, which is far less than 2.0 MPa abs. There is a significant margin between the RCP [RCS] pressure when RPV failure and 2.0 MPa abs. The detailed analysis results can be found in Reference [74].

13.5.6.1.3.2 ATWS

a) Case 4

For this scenario, assuming no SADVs can be used, only the PSVs can be used to depressurise the primary pressure by opening automatically when the primary pressure increases to its threshold value.

According to the analysis results, the primary pressure is 15.9 MPa abs. at the moment

of RPV failure, which is far more than 2.0 MPa abs. This result reveals that the primary pressure cannot be depressurised to lower than 2.0 MPa abs. before RPV failure only with PSVs by opening automatically when primary pressure increases to the threshold value. Detailed analysis results can be found in Reference [74].

b) Case 5

For this scenario, the SADVs are opened when core outlet temperature exceeds 650 °C, and the primary pressure drops quickly after the SADV be opened. According to the analysis results, the primary pressure is 0.28 MPa abs. at the moment of RPV failure, which is far less than 2.0 MPa abs. There is a significant margin between the RCP [RCS] pressure when RPV failure and 2.0 MPa abs. The detailed analysis results can be found in Reference [74].

c) Case 6

For this scenario, the opening time of SADVs is delayed by 30 minutes after the core outlet temperature reaches 650°C, and the primary pressure drops quickly after the SADV are opened.

According to the analysis results, the primary pressure is 0.28 MPa abs. at the moment of RPV failure, which is far less than 2.0 MPa abs. There is a significant margin between the RCP [RCS] pressure when RPV failure and 2.0 MPa abs. The detailed analysis results can be found in Reference [74].

13.5.6.1.4 Conclusion

As the dedicated measures for severe accident mitigation, the SADVs are designed to convert high pressure core melt scenarios to low pressure scenarios with a high reliability.

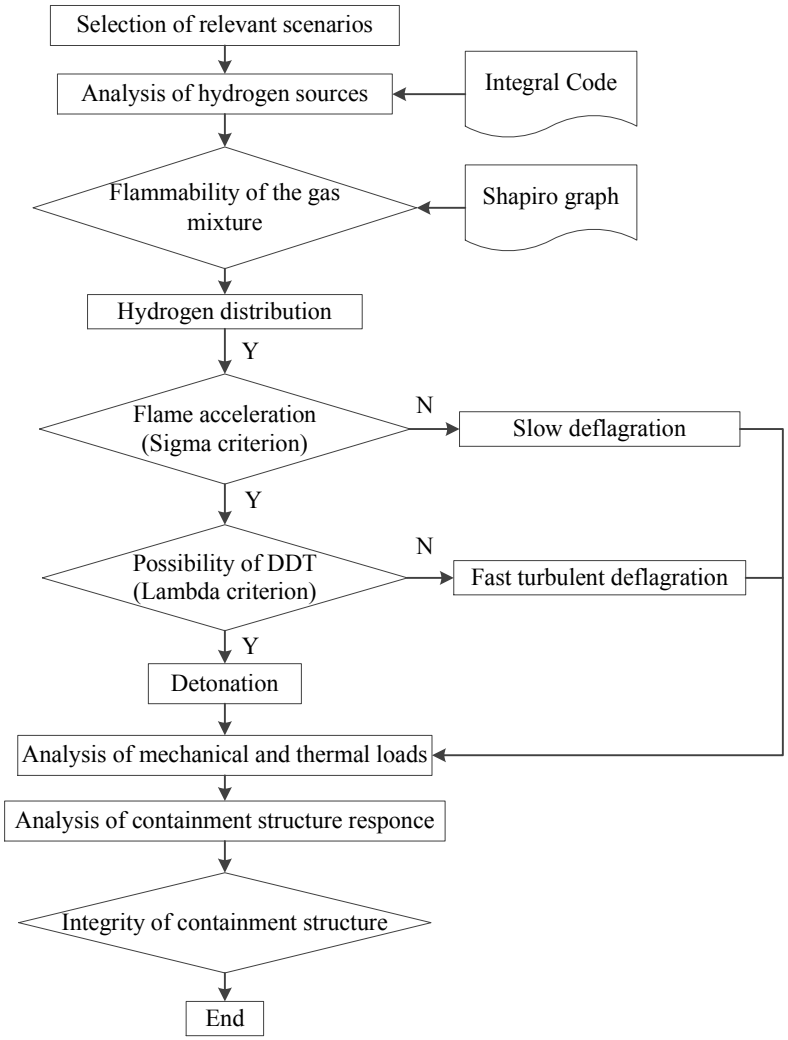
According to the analysis results, the design of SADV can meet the design basis and effectively eliminate the risk of high pressure core melt.

13.5.6.2 Assessment of the EUH [CCGCS]

13.5.6.2.1 Method for the Assessment of the EUH [CCGCS]

Considering the chemical characteristics of combustible gases, the assessment of hydrogen risk in the UK HPR1000 containment includes all the chemistry aspects such as the mass and energy release into the containment, gas distribution and combustion mode, pressure loads from slow deflagration and assessment of risk of DDT. If the flame acceleration cannot be excluded, determination of the pressure loads of the combustion process induced by fast deflagration is performed.

Several steps are taken to assess the EUH [CCGCS] and hydrogen risk, the analysis flow-chart is shown as follows [75] [76]:



F-13.5-10 Flow-chart of the EUH [CCGCS] assessment

(1) According to the PSA results and engineering experience, a set of relevant accident sequences are selected to verify the effectiveness of EUH [CCGCS]. The initiating events of SB-LOCA, IB-LOCA, LB-LOCA and SBO are analysed.

(2) Evaluation of the gas sources for the postulated severe accidents. This step is conducted by analysing several accident scenarios with ASTEC code. The delay of depressurisation is considered to slow down the accident progress and to maximise the hydrogen generation. Preliminary study of the flammability of the mixture gases is also performed.

When the hydrogen concentration is above 10 vol% by volume, flame acceleration may occur. As the local distribution is critical for the flame propagation, a more sophisticated CFD code, GASFLOW, is applied.

The GASFLOW code takes mass and energy release from primary system as an input (ASTEC results) and performs the following assessments:

(3) Evaluate the gas distribution and assess the performance of PARs.

(4) Assess the possibility of Flame Acceleration by the Sigma criteria. If the Flame Acceleration cannot be excluded explicitly, pressure loads induced by fast deflagration are calculated to assess the integrity of the containment.

(5) Assess the possibility of DDT by the Lambda criteria. If the DDT cannot be excluded explicitly, pressure loads induced by DDT are calculated and applied to assess the integrity of the containment.

Typical severe accident sequences are selected and the evaluation of the gas source is performed based on the ASTEC code for step (1) and (2), which is presented in the report *Assessment of containment combustible gas control system by lumped parameter method*, Reference [75]. Based on the ASTEC study, a representative case with a higher potential hydrogen risk is analysed in detail by GASFLOW. The GASFLOW study for the step (3) to (5) is presented in the report *Assessment of EUH [CCGCS] by CFD method*, Reference [76].

13.5.6.2.2 Selection of Relevant Scenarios

In the design of the EUH [CCGCS] in the UK HPR1000, good practice (such as the scenarios selection) is taken into account from the reference plant, where sensitivity analyses on the accident scenarios have been performed to study the hydrogen generation characteristics. In the sensitivity studies of reference plant, severe accidents initiated by not only LOCAs but also SBO are considered. SB-LOCA, IB-LOCA and LB-LOCA with varied locations and varied break areas are studied. LOCAs with different break locations at the cold leg, hot leg and the top of pressuriser are considered. The SBOs are considered because the sequence is slow and the hydrogen releases from the SADVs only. Furthermore, scenarios with delayed depressurisation are also studied. The secondary side cooling which has two-biased effects is also studied. It not only slows down the accident progression and thus the hydrogen production time scale, but also reduces the water vapour generated which is against for inert conditions.

The hydrogen risks in the containment are described as follows:

1) Global risks can be caused by hydrogen slow combustion. Hydrogen slow combustion can lead to a quasi-static load in the containment. This can be bounded by the Adiabatic Isochoric Complete Combustion in the containment. The Adiabatic Isochoric Complete Combustion pressure is calculated for all scenarios. For all scenarios, the Adiabatic Isochoric Complete Combustion pressure remains below the containment design pressure of the UK HPR1000.

2) Local risks can be caused by hydrogen fast deflagration or detonation. Fast deflagration and detonation can lead to dynamic pressure loading which poses a potential threat to the integrity of the containment. The main parameters affecting local risks include hydrogen generation rate (which can lead to high local hydrogen concentration), steam concentration and hydrogen release mode.

Based on the sensitivity studies from the reference plant and the consideration of key parameters for hydrogen risk, 7 scenarios are selected out for the scenarios study in the UK HPR1000. They are listed as follows:

1) Double-ended guillotine LOCA in the cold leg.

   In this scenario, it is assumed that double-ended guillotine LOCA occurs in the cold leg. MHSI and LHSI are unavailable.

2) 5.0 cm (20 cm^2) SB-LOCA at the top of the pressuriser with MCD and LCD.

   In this scenario, it is assumed that 5.0 cm (20 cm^2) SB-LOCA occurs at the top of pressuriser. MHSI and LHSI are unavailable. MCD and LCD are available.

3) 7.5 cm (44 cm^2) IB-LOCA at the top of the pressuriser with MCD and LCD.

   In this scenario, it is assumed that 7.5 cm (44 cm^2) IB-LOCA occurs at the top of pressuriser. MHSI and LHSI are unavailable. MCD and LCD are available.

4) SBO with delay depressurisation of 30 minutes.

   In this scenario, it is assumed that LOOP combined with the loss of the emergency diesel generators occurs. SBO diesel generators are unavailable, MHSI and LHSI are unavailable, secondary heat removal systems are unavailable, SADV is available with a delay in opening of 30 minutes.

5) 5.0 cm (20 cm^2) SB-LOCA in the cold leg with MCD and delay depressurisation of 30 minutes.

   In this scenario, it is assumed that 5.0 cm (20 cm^2) SB-LOCA occurs in the cold leg. MHSI and LHSI are unavailable. MCD is available. SADV is available with a delay open of 30 minutes.

6) 5.0 cm (20 cm^2) SB-LOCA in the hot leg with MCD and delay depressurisation of 30 minutes.

   In this scenario, it is assumed that 5.0 cm (20 cm^2) SB-LOCA occurs in the hot leg. MHSI and LHSI are unavailable. MCD is available. SADV is available with a delay open of 30 minutes.

7) 7.5 cm (44 cm^2) IB-LOCA at the top of the pressuriser with MCD and delay depressurisation of 30 minutes.

   In this scenario, it is assumed that 7.5 cm (44 cm^2) IB-LOCA occurs at the top of pressuriser. MHSI and LHSI are unavailable. MCD is available. SADV is available with a delay open of 30 minutes.

Regarding to hydrogen generation rate, Adiabatic Isochoric Complete Combustion pressure, peak hydrogen concentration of compartments and hydrogen release mode, three scenarios are selected to perform a detailed analysis.

a. 7.5 cm (44 cm^2) IB-LOCA at the top of the pressuriser with MCD and delay depressurisation of 30 minutes

   This scenario leads to a higher hydrogen generation rate. In this scenario, hydrogen releases to pressuriser compartment and reactor coolant pump compartment of loop 2 from break and SADVs. The peak hydrogen concentration in the pressuriser compartment exceeds 10 vol%, which indicates the existence of hydrogen risk in the pressuriser compartment. This scenario leads to an Adiabatic Isochoric Complete Combustion pressure of 0.402 MPa.

b. 5.0 cm (20 cm^2) SB-LOCA at the top of the pressuriser with MCD and LCD

   This scenario leads to a very large amount of hydrogen production, which is 628 kg. Hydrogen releases to pressuriser compartment from the break. The peak hydrogen concentration in pressuriser compartment exceeds 10 vol%, which indicates the existence of hydrogen risk in the pressuriser compartment.

c. SBO with delay depressurisation of 30 minutes

   This scenario leads to a largest amount of hydrogen production, which is 673 kg. Hydrogen releases to the reactor coolant pump compartment of loop 2 from SADVs. This scenario leads to an Adiabatic Isochoric Complete Combustion pressure of 0.483 MPa.

Based on the ASTEC study, a representative case of 7.5 cm (44 cm^2) IB-LOCA at the top of the pressuriser with MCD and delay depressurisation of 30 minutes with higher potential hydrogen risk is analysed in detail by GASFLOW.

13.5.6.2.2.1 7.5 cm (44 cm^2) IB-LOCA at the Top of the Pressuriser with MCD and Delay Depressurisation of 30 min

In IB-LOCA, the coolant discharges from the break to the containment when the accident occurs. Because of the failure of safety injections, the core uncovers and core temperature increases. A large amount of hydrogen is generated by the zirconium-water vapour reaction when the cladding temperature exceeds the threshold values. Hydrogen releases to the pressuriser compartment from the break.

The initial conditions for IB-LOCA are described as follows:

a) The reactor initially operates at state A.

b) A break of diameter 7.5 cm (about 44 cm^2) occurs in the cold leg.

The related assumptions for the IB-LOCA are listed as follows:

a) RIS accumulator available.

b) MHSI unavailable.

c) LHSI unavailable.

d) Containment spray system unavailable.

e) MCD available.

f) IVR available.

g) SADV available with a 30 minutes delay.

13.5.6.2.2.2 5.0 cm (20 cm^2) SB-LOCA at the Top of the Pressuriser with MCD and LCD

In SB-LOCA, the coolant discharges from the break to the containment when the accident occurs. Because of the failure of safety injections, the core uncovers and core temperature increases. Cladding temperature increases and hydrogen is produced by the reaction of zirconium with water vapour. Hydrogen releases to the pressuriser compartment from the break.

The initial conditions for SB-LOCA are described as follows.

a) The reactor initially operates at state A.

b) A break of diameter 5 cm (about 20 cm^2) occurs in the cold leg.

The related assumptions for the SB-LOCA are listed as follows.

a) RIS accumulator available.

b) MHSI unavailable.

c) LHSI unavailable.

d) Containment spray system unavailable.

e) ASG [EFWS] available.

f) MCD available.

g) LCD available.

h) IVR available.

i) SADV unavailable.

13.5.6.2.2.3 SBO with Delay Depressurisation of 30 minutes

In the SBO severe accident, SBO occurs and combines with failure of SBO diesel generators. All of the active safety injection and secondary side safety system are lost due to SBO and loss of SBO diesel generators. The core temperature increases because of loss of cooling. When the core outlet temperature reaches 650 °C, the SADV is opened manually with a 30 minutes delay for primary depressurisation. Cladding temperature increases quickly and hydrogen is produced by the reaction of zirconium with water vapour. Hydrogen is released to the quench tank through

SADVs and finally goes to the reactor coolant pump compartment in the containment.

Initial conditions for the accident analysis are described as follows:

a) The reactor initially operates at state A.

b) The sequence is initiated by LOOP with the loss of the emergency diesel generators.

The related assumptions for the accident analysis are listed as follows:

a) SBO diesel generator unavailable.

b) RIS accumulator available.

c) MHSI unavailable.

d) LHSI unavailable.

e) ASG [EFWS] unavailable.

f) ASP [SPHRS] unavailable.

g) Containment spray system unavailable.

h) IVR available.

i) SADV available with a 30 minutes delay.

13.5.6.2.3 Effectiveness of Mitigation Measures by Lumped Parameter Method

A preliminary study of the effectiveness of the EUH [CCGCS] is performed by ASTEC code. Hydrogen is generated in the core and released from the breaks or the SADVs to its joint compartments. These compartments often have the peak hydrogen concentration. The present study is focused on the hydrogen risks in these main compartments.

13.5.6.2.3.1 7.5 cm (44 cm^2) IB-LOCA at the Top of the Pressuriser with MCD and Delay Depressurisation of 30 min

For this scenario, hydrogen released to the containment can be reduced effectively by EUH [CCGCS] in the long term. Hydrogen releases to the pressuriser compartment and reactor coolant pump compartment of loop 2 through pressuriser break and SADVs. The PARs are passive and can start up automatically during severe accidents. In the scenario, hydrogen generated in-vessel is about 475 kg in total. 380 kg hydrogen, which is about 80 % of the total in-vessel hydrogen production, is effectively recombined by PARs in approximately 50000 s.

a) Without EUH [CCGCS]

For this scenario without EUH [CCGCS], hydrogen released to the containment cannot be reduced. After 4000 s, a large amount of hydrogen starts to release to the

pressuriser compartment due to the rapid cladding oxidation. The peak hydrogen concentration in this compartment is approximately 13.3 vol%. After the SADVs are opened, hydrogen also starts to release to the reactor coolant pump compartment of loop 2 through SADVs. The peak hydrogen concentration in this compartment is approximately 6.3 vol%. In the long term, hydrogen transports to neighbouring compartments and the evaporation of water injected by IVR in cavity leads to the increase of steam, hence the hydrogen concentration in the compartment decreases. The hydrogen concentration is lower than 4 vol% at 50000 s.

The density of hydrogen is smaller than that of air or water vapour, thus the hydrogen tends to flow upward and accumulates in containment large space due to buoyancy. The hydrogen concentration in the containment dome increases slowly. The peak hydrogen concentration in the containment dome is only 4.8 vol% at approximately 22500 s. Then the water in the cavity is heated by the decay heat in the RPV and evaporates. The steam increases in the containment and hydrogen concentration decreases. The hydrogen concentration is lower than 4 vol% at 50000 s, which is approximately 3.14 vol%.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], hydrogen releases to the containment can be reduced effectively in the long term. The pressuriser compartment and reactor coolant pump compartment of loop 2 are the compartments where the hydrogen directly releases. It is not obvious for the PARs to reduce the peak hydrogen concentration due to temporarily high hydrogen generation rate. For pressuriser compartment, the peak hydrogen concentrations still exceeds 10 vol%, which is approximately 13.3 vol%. For the reactor coolant pump compartment of loop 2, the peak hydrogen concentration is approximately 5.4 vol%. In the long term, the hydrogen concentration is lower than 4 vol% due to hydrogen recombination by the PARs.

13.5.6.2.3.2 5.0 cm (20 cm^2) SB-LOCA at the Top of the Pressuriser with MCD and LCD

For this scenario, hydrogen releases to the containment can be reduced effectively by EUH [CCGCS] in the long term. Hydrogen can releases to pressuriser compartment through pressuriser break. The PARs are passive and can start up automatically during severe accidents. In the scenario, hydrogen generated in-vessel is approximately 628 kg in total. 555 kg hydrogen, which is approximately 88 % of total in-vessel hydrogen production, is effectively recombined by PARs in approximately 200000 s.

a) Without EUH [CCGCS]

After 156000 s, a large amount of hydrogen starts to release to the pressuriser compartment due to rapid cladding oxidation. The peak hydrogen concentration in this compartment is approximately 11.4 vol% at 161000 s. Then hydrogen concentration starts to decrease because hydrogen transports to neighbouring

compartments and the water injected by IVR evaporates leading to the increase of steam. The hydrogen concentration in the compartment decreases but remains above 4 vol% at 200000 s.

Hydrogen tends to flow upward. Finally, hydrogen disperses into the large open space and the containment dome. The hydrogen concentration in the containment dome increases slowly. The peak hydrogen concentration in the containment dome is approximately 8.5 vol% at 170000 s. Then water in the cavity is heated by the decay heat in RPV and evaporates. The steam increases in the containment and hydrogen concentration decreases but remains above 6 vol% at 200000 s.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], hydrogen released to the containment can be reduced effectively in the long term. The pressuriser compartment is the compartment where the hydrogen directly releases. It is not obvious for the PARs to reduce the peak hydrogen concentration due to temporarily high hydrogen generation rate. The peak hydrogen concentration still exceeds 10 vol%, which is approximately 10.3 vol%. In the long term, the hydrogen concentration is lower than 4 vol% due to hydrogen recombination by the PARs.

The peak hydrogen concentration is only 5.2 vol% and is lower than 4 vol% in the long term.

13.5.6.2.3.3 SBO with Delay Depressurisation of 30 min

For this scenario, hydrogen releases to the containment can be reduced effectively by the EUH [CCGCS] in the long term. After the SADVs are opened, hydrogen releases to the pressuriser relief tank. Since the pressuriser relief tank is connected to the reactor coolant pump compartment of loop 2 through the pressuriser relief pipeline, hydrogen releases to the reactor coolant pump compartment of loop 2. The PARs are passive and can start up automatically during severe accidents, hence the remaining hydrogen mass in the containment decreases in this scenario with the EUH [CCGCS]. In the scenario, hydrogen generated in-vessel is approximately 673 kg in total. 557 kg hydrogen, approximately 83 % of hydrogen production in-vessel, is effectively eliminated by PARs in ~50000 s.

a) Without EUH [CCGCS]

For this scenario without EUH [CCGCS], hydrogen releases to the containment cannot be reduced effectively. Hydrogen releases to the main coolant pump compartment of loop 2 through SADVs and accumulates in the compartment. After 16000 s, a large amount of hydrogen starts to release to the main coolant pump compartment of loop 2 due to rapid cladding oxidation. The hydrogen concentration in the main coolant pump compartment of loop 2 starts to increase and the peak hydrogen concentration in this compartment is approximately 7.5 vol%. In the long

term, hydrogen transports to neighbouring compartments and the evaporation of water injected by IVR in cavity leads to the increase of steam, hence the hydrogen concentration in the compartment decreases but remains above 4 vol% at 50000 s.

The peak hydrogen concentration in the containment dome is approximately 6 vol%. The hydrogen concentration still exceeds 4 vol% in the long term.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], the main coolant compartment of loop 2 is the compartment where the hydrogen directly releases. It is not obvious for the PARs to reduce the peak hydrogen concentration due to temporarily high hydrogen generation rate. The peak hydrogen concentration is approximately 6.7 vol%. In the long term, the hydrogen concentration is lower than 4 vol% due to hydrogen recombination by the PARs.

The hydrogen in the containment dome is recombined effectively by PARs. The peak hydrogen concentration is approximately 4.3 vol% and is lower than 4 vol% in the long term.

During the above analysis, the PARs are assumed to be 100% efficient. Sensitivity analysis on the recombination of hydrogen and hydrogen distribution will be performed to study the uncertainties. The analysis will be submitted in the report *Sensitivity studies on key parameters of hydrogen risk assessment* before December 2020.

13.5.6.2.4 Effectiveness of Mitigation Measures by CFD Code

When the hydrogen concentration is above 10 vol% by volume, flame acceleration may occur. Based on the ASTEC analysis, the peak hydrogen concentration is higher than 10 vol% in pressuriser compartment for 7.5 cm (44 cm^2) IB-LOCA at the top of the pressuriser with MCD and delay depressurisation of 30 minutes and 5.0 cm (20 cm^2) SB-LOCA at the top of the pressuriser with MCD and LCD. Due to the higher peak hydrogen concentration, the scenario of 7.5 cm (44 cm^2) IB-LOCA at the top of the pressuriser is selected as the bounding case for CFD analysis.

The initial and boundary conditions are obtained from the ASTEC code. The hydrogen inventory is multiplied deliberately to equivalent to the hydrogen generation by 100% zirconium oxidation in the active core region.

The gas mixture could develop a homogenous distribution in the containment even with asymmetric injection during the process of accident.

For the performance of the PARs, the PARs manage to control the containment concentration below 10 vol% in a conservative hydrogen release assumed in this report. The heat release from the PARs has limit effect on the thermal- hydraulics of the containment. The setup of the sensors is representative on capturing the main flow behavior of hydrogen transport in the open space.

The flame acceleration cloud only exists in the distinct and relatively short phase during the hydrogen release period with a limited amount of hydrogen inventory. During all other times, the flame acceleration can be excluded for the entire containment. The DDT can be safely excluded for the containment during the whole process of accident.

13.5.6.2.5 Conclusions

The assessment of the EUH [CCGCS] is performed thoroughly for the UK HPR1000. Based on the assessment by the integral code ASTEC, the Adiabatic Isochoric Complete Combustion pressure remains below the containment design pressure of UK HPR1000. The hydrogen concentration in the compartment where hydrogen releases and the containment dome is lower than 4 vol% in the long term. It is concluded that the global hydrogen risk can be mitigated effectively by EUH [CCGCS].

Based on the study by CFD method, the DDT can be safely excluded for the containment during the whole process of accident. The flame acceleration cloud only exists in the distinct and relatively short phase during the hydrogen release period with a limited amount of hydrogen inventory. Pressure loads induced by slow deflagration or flame acceleration will be assessed in the updated version report *Assessment of EUH [CCGCS] by CFD method (GHX00600298DRAF02G, Rev. C, submitted before 31/05/2020*), to evaluate the threat to the integrity of containment. The assessment of EUH [CCGCS] for the reference plant shows that the hydrogen explosion risk can be prevented and the integrity of the containment is not threatened.

13.5.6.3 Assessment of IVR

13.5.6.3.1 Assessment Method

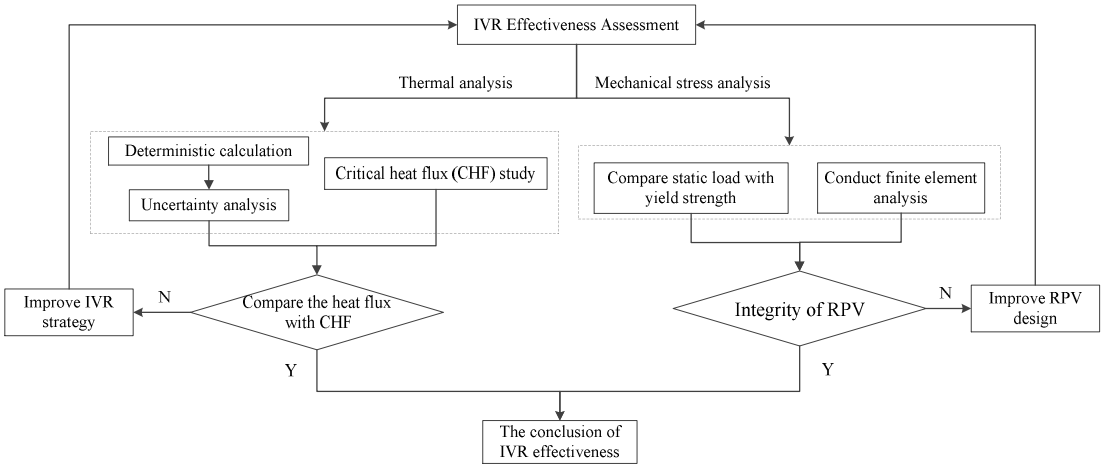
To ensure that IVR strategy is effective after severe accidents, the following criteria are required to be met:

a) The heat flux transferred from the corium to the outer surface of RPV lower head must be lower than the local CHF, namely the RPV wall cannot be melted through in steady state.

b) When part of the RPV lower head wall has been ablated by molten corium, the minimum thickness still has enough mechanical strength to maintain the RPV integrity.

When the core outlet temperature reaches 650°C, after the RCP [RCS] is depressurised, the valves between the IVR tank and the cavity are opened to passively inject water into reactor pit in order to remove the decay heat from the lower head of RPV.

Thermal analysis and mechanical stress analysis are both taken into consideration to assess the effectiveness of IVR, the analysis flow-chart is shown in F-13.5-11.



F-13.5-11 Flow-chart of the IVR assessment

In order to demonstrate the effectiveness of the IVR, three issues should be considered. Firstly, the heat flux from the corium pool to RPV wall is obtained. Secondly, a series of IVR related tests are performed to obtain the CHF distribution along the outer surface of RPV. Finally, the mechanical analysis is conducted to evaluate whether the residual wall can sustain the integrity of RPV. The details are described as follows.

a) Deterministic analysis: A series of severe accident sequences which will lead to core damage are identified by PSA, deterministic analysis and engineering judgement. The initiating events of LB-LOCA, IB-LOCA, SB-LOCA and SBO with loss of SBO diesel generators have been calculated.

b) Critical heat flux study: IVR experiments have been conducted to obtain the CHF distribution along the RPV outer surface.

c) Uncertainty analysis on thermal load: In order to carry out the uncertainty analysis on heat flux which transfers from corium pool to RPV wall, a dedicated code, MOlten POoL (MOPOL), is employed. The four key parameters which affect the heat transfer in corium pool are studied, which are decay heat in molten pool, fraction of Zr oxide, mass of Fe, fraction of reactor core melt. A Probability Density Function (PDF) for the key parameters is confirmed and substantial heat flux results are obtained by different input parameters.

d) Mechanical stress analysis: There are two major approaches to study the mechanical stress. The first one is comparing static load with yield strength. This is a simple method to evaluate whether the residual wall can keep the integrity of RPV. The second one is finite element analysis. This is a complex method to evaluate the minimum thickness of RPV which can maintain the integrity of RPV with considering the creep deformation or other factors.

13.5.6.3.1.1 Method of Deterministic Analysis

Different severe accident sequences which will lead to core damage should be identified by PSA and calculated with different conservative conditions so that the safe margin for different kinds of severe accidents can be identified.

It is reasonable to select the different kinds of severe accident scenarios to verify the effectiveness of IVR. According to PSA and engineering judgments, the initiating events of LB-LOCA type, IB-LOCA type, SB-LOCA type, ATWS type and SBO with loss of SBO diesel generators should be analysed. The assumptions of other safety systems functions with conservative consideration are as follows:

a) The accumulators act automatically once the primary pressure lowers to its threshold.

b) MHSI, LHSI and the containment spray are unavailable.

c) IVR is available.

Calculations with different kinds of severe accident scenarios are done by ASTEC.

According to the result of different types of severe accident scenarios, the accident progression, typical severe accident phenomena, the variation of primary system pressure and primary system temperature, the decay heat of molten pool in the lower plenum, the compositions of the corium pool and the residual wall thickness of the lower head of RPV, etc. are obtained through the calculation of ASTEC. The residual thickness of the lower head can be obtained to evaluate the integrity of RPV. The pressure difference between inside and outside of RPV can be obtained, which can be used to conduct mechanical stress analysis. The decay heat and the compositions of corium pool can also be obtained to conduct the uncertainty analysis.

13.5.6.3.1.2 Method of Uncertainty Analysis on Thermal Load

Even though the deterministic analysis results can be obtained based on several types of severe accident sequence calculations, we cannot calculate all the severe accident sequences with different initial accident conditions and different mitigation measures. Especially, in severe accidents, the corium will finally collapse into the RPV lower head. The progress is complex and there are many uncertainties on the oxidation fraction of core melt, decay heat, etc. When the inherent heat flux density transfer from the corium pool to the RPV outer surface is calculated, the Risk Oriented Accident Analysis Methodology (ROAAM) is adopted to analyse these uncertainties on thermal load. In order to carry out the uncertainty analysis on heat flux which transfers from corium pool to RPV wall, based on ROAAM, the MOPOL code is employed to calculate this local heat flux. It should be noted that the IVR effectiveness analysis mainly depends on the ASTEC calculation for the transient process with different severe accident sequences and function assumptions. The MOPOL code is a supplementary method to perform uncertainty analysis of heat

transfer in the corium pool based on two assumptions. One of these assumptions is that the molten pool has the configuration of two different layers, which means the metallic layer is above the oxide layer. Another assumption is that the molten pool has reached its steady thermal state, which means the volume of corium generating heat has been maximised. The details are described as follows.

The two-layer heat transfer models of the corium pool were adopted in the analysis. The corium pool structure is:

a) An oxide layer (solid oxide crust and molten oxide layer) composed of all the core oxide fragments in the lower head in hot steady state.

b) A molten metal layer at the top of the crust on the oxide layer consists of all "light" components (reflector, core support plate, part of core barrel and lower internal structures) in the core area.

The main heat transfer mode of the corium pool is natural convection, so it is called "stable natural convection corium pool". The assumed characteristics of the stable natural convection corium pool are:

a) The components of the oxide layer mainly include UO_2 and ZrO_2, with a melting point approximately of 2973 K. The oxide layer is surrounded completely by crust.

b) The temperature of the crust boundaries is equal to the melting point of the corium.

c) The lateral surface of the metal layer is almost vertical. The metal layer is heated on its lower surface and releases heat through its upper and lateral surfaces. The temperature of its lateral surfaces is the metal melting point (approximately 1600K).

d) The natural convection in the metal layer is expressed as Rayleigh number Ra and that in the oxide layer is expressed as "internal Rayleigh number" $Ra'=RaDa$. $Da=H^2Q/k(T_{max}-T_i)$ is used to express the volumetric internal heat source, where Q represents the volumetric heat release rate, H represents the characteristic height, k represents the heat conductivity, T_{max} and T_i respectively represent the maximum temperature and boundary temperature.

The main inputs for calculating heat transfer in the corium pool include:

a) The geometry parameters of the RPV lower head.

b) The mass of molten stainless steel, the fraction of oxidised zirconium, the fraction of molten core, and the decay heat of the corium pool.

13.5.6.3.1.3 Method of Critical Heat Flux Study

Heat transfer from the RPV outer surface to water in the reactor pit is mostly

restricted by the local critical heat flux. The heat-transfer mechanism of the outer surface of the RPV is nucleate boiling at the beginning. With increase of the heat flux, nucleate boiling may turn to film boiling. At this time, the heat flux transferred from the outer face to cooling water drops sharply, so that the capacity of cooling decreases quickly. There are many factors which can affect the CHF, such as the flow rate of natural circulation, the layout of metal insulation, etc. By conducting the IVR test to simulate the heat transfer process, the CHF distribution can be obtained.

The success criterion of the IVR strategy is that the actual heat flux on the outer surface of the RPV lower head is lower than the local critical heat flux.

13.5.6.3.1.4 Method of Mechanical Stress Analysis

The SADVs are used for primary loop depressurisation after severe accidents. In order to evaluate whether the residual thickness can keep the integrity of RPV when a corium pool forms, the mechanical stress calculation has been conducted.

If the initiating sequence of a severe accident is a lower pressure initiating event, such as LB-LOCA or IB-LOCA, even if the SADV does not open, the pressure of the primary system decreases rapidly, and the pressure difference between the inner and outer of the primary loop can be neglected when the corium pool forms. If the initiating sequence is one of the high pressure accidents, such as SB-LOCA, SBO, etc., the pressure difference between the inner and outer of the primary loop also decreases rapidly after the SADV is opened. So the pressure difference between inner and outer of RPV can be neglected when conducting the mechanical stress analysis.

As shown in the above flowchart, there are mainly two methods to conduct the mechanical stress analysis. The first one is the method of static load-yield strength. According to the results of severe accidents which have been studied, the static load includes the mass of lower support plate, baffle, flow distribution device, a certain mass of the core barrel, the whole core and the mass of the RPV lower head. The buoyancy of the RPV should also be considered. The yield strength can be obtained from the physical test results of RPV. Thus the minimum area (A_r) required for bearing this static load is:

$$A_r = \frac{Static - Load}{Yield - Strength}$$

The actual minimum thickness can be calculated by using the Fourier 1D heat conductivity formula. The safety margin of mechanical stress can be evaluated by comparing the actual minimum thickness with the critical thickness for bearing the static load.

According to the present study, the results show that if the UK HPR1000 implements the IVR strategy, it can achieve a great mechanical stress margin. As for the

mechanical stress analysis, the finite element analysis will be conducted in the following stage. Based on the success criteria for IVR, it can be known that whether it is effective mainly depends on whether the RPV lower head can sustain thermal load successfully or not, namely "local heat flux - critical heat flux criterion", which means that the heat flux on the RPV out surface must be lower than the local critical heat flux.

13.5.6.3.2 Effectiveness Evaluation for In-Vessel Retention Strategy

13.5.6.3.2.1 Deterministic Analysis

To conduct the deterministic analysis and comparison, LB-LOCA is selected as the bounding sequence for IVR evaluation and IB-LOCA, SB-LOCA, SBO and ATWS are analysed as the IVR-related severe accident sequences for sensitivity study. The other safety systems functions assumptions with conservative consideration are as follows:

a) The accumulators act automatically once the primary pressure lowers to related threshold.

b) MHSI, LHSI and the containment spray are unavailable.

c) IVR is available.

For LB-LOCA, after the relocation of corium into lower head, the maximum heat removal from the outer surface of the vessel is located near the top of the molten pool. The results show that the transient heat removal is smaller than the CHF during the transient process after the relocation. And when the heat removal reaches its maximum, the margin between local heat flux and CHF is acceptable for the evaluation. For the residual thickness of the vessel wall, the minimum residual thickness of lower head wall is 0.0415 m at the azimuth from 78° to 87° and according to the mechanic load analysis, it is concluded that the RPV can maintain its integrity during LB-LOCA scenario.

For IB-LOCA, the maximum heat removal from the outer surface of the vessel is located near the top of the molten pool and when the heat removal reaches its maximum, the margin between local heat flux and CHF is acceptable for the evaluation. The minimum residual thickness of lower head wall is 0.0415 m at the azimuth from 81° to 87° and according to the mechanic load analysis, it is concluded that the RPV can maintain its integrity during IB-LOCA scenario.

For SB-LOCA, the maximum heat removal from the outer surface of the vessel is located near the top of the molten pool and when the heat removal reaches its maximum, the margin between local heat flux and CHF is acceptable for the evaluation. The minimum residual thickness of lower head wall is 0.0496 m at the azimuth from 81° to 87° and according to the mechanic load analysis, it is concluded that the RPV can maintain its integrity during SB-LOCA scenario.

For SBO plus SBO diesel failure, the maximum heat removal from the outer surface of the vessel is located near the top of the molten pool and when the heat removal reaches its maximum, the margin between local heat flux and CHF is acceptable for the evaluation. The minimum residual thickness of lower head wall is 0.0496 m at the azimuth from 81° to 87° and according to the mechanic load analysis, it is concluded that the RPV can maintain its integrity during SBO plus SBO diesel failure scenario.

For ATWS, the maximum heat removal from the outer surface of the vessel is located near the top of the molten pool and at the timing when the heat removal reaches its maximum, the margin between local heat flux and CHF is acceptable for the evaluation. The minimum residual thickness of lower head wall is 0.0496 m at the azimuth from 78° to 87° and according to the mechanic load analysis, it is concluded that the RPV can maintain its integrity during ATWS scenario.

From the deterministic analysis of LB-LOCA, IB-LOCA, SB-LOCA, ATWS and SBO with loss of SBO diesel generators scenarios, it is concluded that the RPV can maintain its integrity during these five scenarios.

13.5.6.3.2.2 Reactor Vessel External Cooling Tests

The REVECT-II facility was specifically designed and built to study the critical heat flux distribution. The CHF correlation is fitted by the CHF test data of the REVECT-II facility for HPR1000 (FCG3).

13.5.6.3.2.3 Uncertainty Analysis on Thermal Load

Except integral severe accident analysis code, MOPOL is another dedicated code used to evaluate the thermal load uncertainty of IVR based on the steady two-layer model. The input parameters for heat transfer calculation are as follows:

1) Reactor parameters.

2) CHF curve of the RPV outer surface.

3) The mass of molten stainless steel, the fraction of oxidised zirconium, the fraction of molten core and the decay heat of the corium pool.

According to the ROAAM methodology, the analysis target can be deconstructed into a series of "sub-phenomenon" - certainty parameters, randomness parameters and uncertainty parameters, thus laying a general solid foundation for comparison between analysis and opinions of different experts. The key point is the determination of uncertainty parameters. For the solution of heat flux density of the RPV outer surface, the three main uncertainty parameters are:

1) Thickness of metal layer in the corium pool.

2) Volume of oxide layer in the corium pool.

3) Decay heat in the corium pool.

The metal layer mainly includes stainless steel and non-oxidised zirconium. The oxide layer mainly includes UO_2 and ZrO_2. So the above three parameters can be obtained by the following four parameters:

1) Mass of molten stainless steel.

2) Fraction of oxidized zirconium.

3) Fraction of molten core.

4) Decay heat of corium pool.

The ranges of the above four parameters are known by deterministic analysis combined with conservative hypothesis. Then considering the contribution of different severe accident sequences to the CDF, three different levels of likelihood are determined by engineering judgement according to ROAAM, including the very unlikely level (10^{-2}), unlikely level (10^{-1}) and likely level (10^{0}). When the range and the probability are determined, the probability density functions are obtained.

If the above parameters are known, the heat flux of any location on the out surface of RPV lower head can be calculated through the corium pool heat transfer model. The 10000 groups of random sampling that form Probability Density Functions (PDFs) show that there is still a margin between the calculated heat flux and CHF obtained by experiment. The ratio of calculated heat flux to the CHF obtained by experiment of the curve with the maximum heat flux among these 10000 groups is approximately 0.94 which is smaller than 1. However, it should be noted that this curve is an extreme group with the physically impossible values of key parameters. The decay heat for this curve is 26.48 MW. The oxidation fraction of zirconium for this curve is 69.69 % and the mass of stainless steel is 48.13 t. It is physically impossible for a case to have not only a large decay heat but also a large oxidation fraction of zirconium. From uncertainty analysis, the margin between the local heat flux and the CHF is acceptable.

13.5.6.3.2.4 Mechanical Stress Analysis

The input parameters for mechanical stress analysis are as follows: 1) Weights of different components inside RPV; 2) Yield strength of RPV steel; 3) Environmental conditions under severe accident; 4) Conservative assumption of heat flux; 4) Other material properties of RPV steel.

For the static load analysis, the results show that when the heat flux reaches 1.8 MW/m^2, the required residual thickness of the RPV is 8.5 mm and the actual minimum thickness of the RPV is 28 times the required minimum thickness for bearing the static load. If the UK HPR1000 implements IVR strategy, it can achieve a significant mechanical stress margin. As for the mechanical stress analysis, more work with finite element analysis should be conducted in the flowing stage. During the injection of water, the outside of the RPV is subjected to thermal shock loading. The

fast fracture analysis for the RPV has been studied when the RPV is subjected to internal pressure loading and thermal shock loading during the injection of water in IVR condition [77]. The thickness of part of the RPV shell is reduced by ablation. Considering the thermal load, dead weight and pressure difference between outside and inside of the RPV, the detailed mechanical assessment will be performed. Based on the success criteria for IVR, it can be deduced that whether it is effective mainly depends on whether or not the RPV lower head can sustain thermal load successfully, namely "local heat flux - critical heat flux criterion", which means that the heat flux on the RPV outer surface must be lower than the local critical heat flux.

13.5.6.3.3 Conclusion

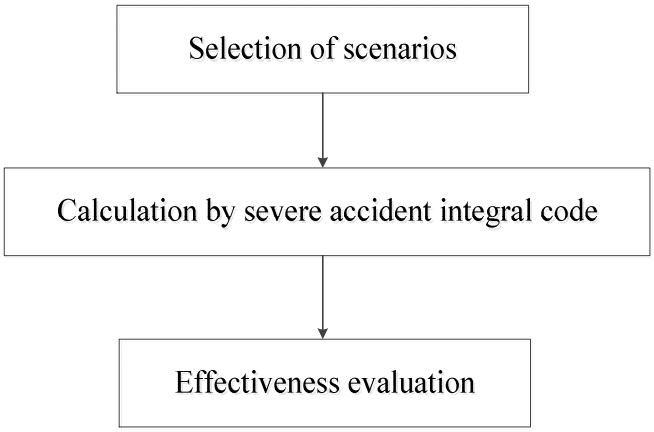
According to the deterministic analysis results of LB-LOCA, IB-LOCA, SB-LOCA, ATWS and SBO severe accident conditions, the decay heat in the lower head of the RPV can be removed by the reactor pit flooding system. Though the minimum residual thickness of RPV wall could reduce to 40 mm, the RPV can still maintain integrity. And the results of uncertainty analysis show that the margin between the calculated heat flux at the steady state and the CHF obtained by experiment is acceptable.

The pressure difference between inner and outer of the primary loop is very small after the steady corium pool is formed. The result of static loads analysis shows that the residual wall thickness can bear the static load. The finite element analysis is presented in the report *The Structural Integrity Assessment of RPV on In-Vessel Retention Condition* [78].

13.5.6.4 Assessment of the EHR [CHRS]

13.5.6.4.1 Assessment Process

The assessment of the EHR [CHRS] consists of the following steps. And the analysis flow-chart is shown as follows:



F-13.5-12 The flow-chart of the EHR [CHRS] assessment

1) Step 1: A set of relevant accident sequences are selected according to the PSA

results and engineering experience.

2) Step 2: Calculation of the containment pressure and temperature for the postulated severe accidents based on severe accident integral code.

3) Step 3: Effectiveness assessment of the EHR [CHRS] based on the acceptance criteria and the calculation results.

13.5.6.4.2 Selection of Scenarios

For assessment of the EHR [CHRS], according to the accident sequence selection results [45], the LB-LOCA in hot leg is chosen. The LB-LOCA in hot leg scenario at power condition is the accident sequence with the fastest accident progression and fastest early-stage pressure increase in the containment because of the large release of coolant at the initial stage.

13.5.6.4.3 Analysis Code

Calculations are performed by ASTEC, and the description of the code is given in Appendix 13A.

13.5.6.4.4 Acceptance Criteria

During the assessment of the EHR [CHRS], 12 hours after the severe accident, the EHR [CHRS] is started and the pressure in the containment begins to drop due to the spray. The acceptance criteria of the effectiveness assessment are the same as those listed in Sub-chapter 13.5.5.4.2. The effectiveness of the EHR [CHRS] can be justified by comparing the calculation results to the design basis.

13.5.6.4.5 Effectiveness Evaluation for EHR [CHRS]

13.5.6.4.5.1 Initial Conditions and Main Assumptions

The initial conditions for the accident analysis are as follows.

1) The Initial reactor operation condition is at the full power condition.

2) A double-ended break occurs at the primary hot leg.

Considering that more mass and energy is released into the containment, the related assumptions for the accident analysis are as follows.

1) MHSI and LHSI are unavailable.

2) All accumulators are available.

3) IVR is manually actuated with 20 minutes delayed after the core outlet temperature reaches 650°C.

4) Two trains/one train of the EHR [CHRS] are manually started to remove the heat in the containment 12 hours after the core outlet temperature reaches 650°C.

There is enough time for manual actuation due to the 12-hour grace period. Furthermore, for most fault scenarios, even without EHR [CHRS], the containment design pressure will not be reached within 24 hours providing additional time to allow emergency response.

5) The inlet water temperature of the cold side (heat sink) in the EHR [CHRS] is 45°C, and its flowrate is 360 m³/h. If two trains of the EHR [CHRS] are manually started, the flowrate of the hot side for one train is 330 m³/h (290 m³/h for spray, 40 m³/h for active reactor pit water injection), and that of the other train is 300 m³/h (300 m³/h for spray). If only one train of the EHR [CHRS] is manually started, the flowrate of the hot side is 330 m³/h (290 m³/h for spray, 40 m³/h for active reactor pit water injection).

13.5.6.4.5.2 Results Analysis

The detailed results for this scenario are presented in Reference [79]. During the whole accident process, the accident progression for the LB-LOCA case without the EHR [CHRS] and with activation of two/one the EHR [CHRS] trains after 12 h are described as follows.

a) LB-LOCA without EHR [CHRS]

1) For this case, steam and water are quickly released into the containment through the break at the initial stage, causing a pressure peak at the beginning of the event.

2) Afterwards, the containment pressure begins to drop gradually due to the decrease in the released quantity of coolant and due to the heat absorption effects of the containment heat structures.

3) After the core outlet temperature reaches 650°C, the IVR strategy has started to flood the reactor pit, decay heat causes the water in the reactor pit to evaporate and releases it into the containment. This results in a gradual pressure rise in the containment for a long time. Eventually the containment pressure reaches the containment design pressure (0.52 MPa abs.), thus leading to containment failure in the long term.

b) LB-LOCA with one train of EHR [CHRS]

1) For this case, the accident progression is the same as the LB-LOCA without EHR [CHRS] scenario before the EHR [CHRS] started.

2) Twelve hours after the core outlet temperature reaches 650°C, one train of EHR [CHRS] are manually started to remove the heat in the containment, which enables the containment pressure to be maintained below the design pressure (0.52 MPa abs.) at any stage. The containment pressure can be reduced to { } within approximately 9516 seconds (2.64 hours) after the EHR [CHRS]

actuation and maintained below { } for long term operation.

c) LB-LOCA with two trains of EHR [CHRS]

1) For this case, the accident progression is the same as the LB-LOCA without EHR [CHRS] scenario before the EHR [CHRS] started.

2) Twelve hours after the core outlet temperature reaches 650°C, two trains of EHR [CHRS] are manually started to remove the heat in the containment. The containment pressure can be reduced to below { } within approximately 2686 seconds (0.75 hours) after the EHR [CHRS] actuation.

13.5.6.4.5.3 Uncertainty Analysis

The calculation results show that there are enough margins in the design of EHR [CHRS] in the UK HPR1000, which can cover the uncertainty from calculation process. These margins are described as follows.

a) In the design of the EHR [CHRS], only the 12-hour grace period is considered. But for most severe accidents, even without the EHR [CHRS], the containment design pressure will not be reached within 24 hours providing enough margin for EHR [CHRS] start-up.

b) According to calculation results, activating two trains of the EHR [CHRS] can reduce the containment pressure below { } within approximately 45 minutes of EHR [CHRS] operation, and activating one train of the EHR [CHRS] can reduce the containment pressure below { } within approximately 2.64 hours of EHR [CHRS] operation. Compared with the acceptance criteria, this provides enough margin.

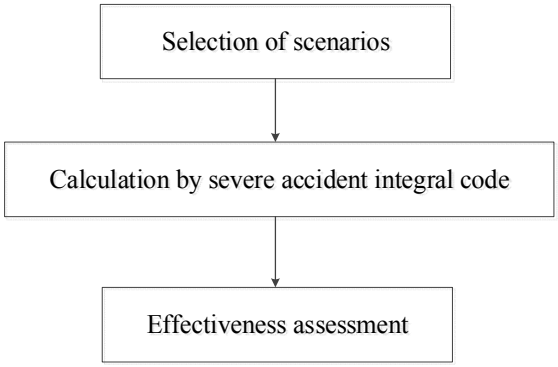
13.5.6.4.6 Conclusions

According to the analysis results [79], the containment pressure remains clearly below the containment design pressure under a LB-LOCA severe accident. The design of the EHR [CHRS] is able to meet the design basis requirements and effectively decrease the pressure in the containment and remove the decay heat in the containment.

13.5.6.5 Assessment of the EUF [CFES]

13.5.6.5.1 Method for the Assessment of the EUF [CFES]

Several steps are taken to assess the EUF [CFES], and the analysis flow-chart is as follows:



F-13.5-13 The flow-chart of EUF [CFES] assessment

a) Selection of relevant scenarios

Extremely unlikely conditions are considered, such as long term loss of all AC power with LB-LOCA (This is conservative, to make containment pressure increase early, assuming LB-LOCA as the initial accident according to the selected sequence in T-13.5-4). Due to long term loss of all AC power, the core begins to melt and containment pressure increases. However, the passive IVR of the EHR [CHRS] is still available and can be implemented by passive flooding from the IVR tank. Before depletion of the IVR tank, the mobile diesel pumps are used for IVR injection. Containment pressure increases due to the sustained evaporation of injection water. When containment pressure has increased to the design pressure, the EUF [CFES] is opened for controlling the containment pressure.

b) Calculation by severe accident analysis code

Calculations are conducted by ASTEC, and the description of the code is given in Appendix 13A.

c) Result analysis

The analysis results are shown in PCSR Sub-chapter 13.5.6.5.4.

13.5.6.5.2 Event Descriptions

As described above, LB-LOCA sequence with long term loss of all AC power is selected and the detailed descriptions are as follows.

The initial conditions for the accident analysis are as follows.

a) Initial reactor operation condition is at the full power condition.

b) Double ended rupture of LB-LOCA occurs.

c) Long term loss all AC power.

The related assumptions for the accident analysis are as follows.

a) RIS accumulator available.

b) ASP [SPHRS] unavailable.

c) MCD unavailable.

d) LCD unavailable.

e) MHSI unavailable.

f) LHSI unavailable.

g) ASG [EFWS] unavailable.

h) Containment spray of the EHR [CHRS] unavailable.

i) Opening of the SADVs when core outlet temperature exceeds 650°C.

j) Passive IVR available.

k) The mobile diesel pumps are used for IVR injection.

l) EUH [CCGCS] available.

m) Open the EUF [CFES] when containment pressure exceeds 0.52 MPa abs.

13.5.6.5.3 Effectiveness of Mitigation Measures

The selected scenario for the EUF [CFES] assessment is conservative to get the earliest containment depressurisation starting time in the long term loss of all AC power accident. It is conservative enough to cover the uncertainty of the containment depressurisation start time.

Calculations are performed by ASTEC, the accident progression for the LB-LOCA case with the EUF [CFES] is described as follows.

In the case of LB-LOCA with long term loss of all AC power, the containment pressure increases due to the steam and non-condensable gas accumulation. At approximately 62h 25min, the containment pressure exceeds 0.52 MPa abs. and operators manually open the containment isolated valve to start up the EUF [CFES]. Twelve hours after continuous operation of the EUF [CFES], the containment pressure decreases sufficiently. Then the EUF [CFES] needs to be closed and refilled. Before the containment pressure increases to the design pressure again, there is sufficient time to replenish the water and chemical inventory of the combined filter unit.

The EUF [CFES] operation time depends on the emergency response actions and the recovery time of electrical power. As the results showed, the increased rate of containment pressure is low in the long term. When EUF [CFES] is needed to open again, it is approximately 4 days after the SA. It is credible that some equipment will be available to control the pressure in the containment at that moment.

Therefore, for the assessment of EUF [CFES], depressurisation capability of EUF

[CFES] covers the uncertainty of operation strategy.

13.5.6.5.4 Conclusions

The calculation on assessment of EUF [CFES] for UK HPR1000 (FCG3) is presented in Reference [80]. The conclusion is that the system capability is adequate to meet the design basis of EUF [CFES]. EUF [CFES] is effective to control containment pressure when containment spray of EHR [CHRS] is unavailable in the long term loss of all AC power accidents.

13.5.7 Source Term Evaluation of DEC-B events

Severe accident source terms presented here are based on the success of the severe accident mitigation strategy. The integrity of containment is maintained by the operation of severe accident mitigation measures. Therefore, fission products release to the environment caused by the leakage of inner containment. The other fission product release categories and scenarios refer to PCSR Chapter 14.

With respect to radiological releases into the environment, the representative initiating sequences for severe accidents are LB-LOCA and LOOP.

The LB-LOCA represents the fastest release of coolant and fission products from the primary system, and provides bounding conditions for the containment pressure. Pressure-driven leakage from the containment therefore results in large release into the Safeguard Building Controlled Area Ventilation System (DWL [SBCAVS]) and Annulus Ventilation System (EDE [AVS]), and finally into the environment.

The LOOP with failure of all diesel generators involves the loss of DWL [SBCAVS] during the first 12 hours, and is therefore associated with an unfiltered ground-level release into the environment. The EDE [AVS], which is linked to the 12 hours UPS, operates during this period. After 12 hours, both DWL [SBCAVS] and EDE [AVS] ventilation systems are switched to the emergency power supply system and filtered release through the stack takes place.

13.5.7.1 Method for the Assessment of Severe Accident Source Terms

ASTEC is used for the assessment of severe accident source terms.

13.5.7.1.1 Core Inventory

In the core inventory modelling in ASTEC, the mass of each nuclide at the End Of Life (EOL) is taken as the initial mass. Then, the mass release fraction of each element is calculated by the code.

In the post-processing of calculation results, the maximum radioactivity of each nuclide in the whole reactor life is taken as the initial radioactivity after accidents.

13.5.7.1.2 Fission Product Behaviour Modelling

The mechanisms of fission product behaviour that are taken into account in the modelling are listed in T-13.5-6, including the formation from vapour phase into aerosols and the aerosol agglomeration, deposition mechanism, etc.

T-13.5-7 Fission Product Phenomena Modelling in the ASTEC

Vapour phase mechanism	
Homogeneous/heterogeneous nucleation	Yes
Vapour condensation on wall	Yes
Vapour sorption on wall	Yes
Aerosol agglomeration mechanism	
Brownian coagulation	Yes
Gravitational coagulation	Yes
Turbulent coagulation	Yes
Aerosol deposition mechanism	
Impaction (bend, contraction, eddy)	Yes
Laminar/turbulent diffusion	Yes
Thermophoresis	Yes
Diffusiophoresis	Yes
Settling	Yes
Aerosol other mechanism	
Pool scrubbing	No
Mechanical resuspension	Yes
Washing down	Yes

Vapour phase mechanism	
Chemistry	
Iodine chemistry	Yes

13.5.7.1.3 Iodine Chemistry Modelling

Iodine chemistry includes gaseous phase chemistry, liquid phase chemistry and mass transfer between gaseous phase and liquid phase. The chemical transformation of iodine is a kinetic process in the containment, taking into account three kinds of reaction: thermal reactions, radiolysis reactions and mass transfer processes. The iodine species involved in the reactions are I_2, CH_3I, I_2O_5, I^-, IO_3^-, HOI and AgI.

a) Dose Rate for Iodine Chemistry Modelling

The radiolysis reaction in the iodine chemistry is estimated under dose conditions, and the dose condition in the containment is calculated by the dose model of ASTEC. The calculation of source term, iodine chemistry and dose are coupled in ASTEC.

b) The Setting of pH for Iodine Chemistry Modelling

According to the design target of pH control measures (which is to keep the pH of IRWST above 7 after accidents 8 hours), and based on the results in section 13.5.7.2, in the setting of pH for iodine chemistry, the pH of IRWST is set at 3.5 in the first 8 hours. After 8 hours, the pH of the IRWST is set at 7.

13.5.7.1.4 Leakage Modelling

The containment design leakage rate is 0.3 vol% (volume) per day at design pressure (0.52 MPa abs.). To be conservative, when the containment pressure is below 0.52 MPa abs., the leakage is assumed to be 0.3 vol% per day in the model. A fraction of 40% of the total containment leakage is assumed to be routed via penetrations to the annulus and 60% to the safeguard building controlled area.

13.5.7.2 pH Assessment

With liquid iodine chemistry, the formation of volatile I_2 in the sump depends on a number of parameters, the most important being the pH. The pH should be alkaline and the rate of production of volatile I_2 will be very low. A Tri-Sodium Phosphate (TSP) adjustment basket is used to control the pH of IRWST sump after accidents.

13.5.7.2.1 pH Modelling

The pH of IRWST sump is analysed by ASTEC in pH stand-alone mode. Chemical species and reactions considered in the pH analysis are listed as follows:

a) Water autoprotolysis.

b) The formation and acidity of carbonic acid (H_2CO_3).

c) The formation and acidity of nitric acid (HNO_3).

d) The acidity of boric acid (H_3BO_3).

e) The dissolution of lithium hydroxide (LiOH).

f) The dissolution of TSP.

13.5.7.2.2 Analysis Assumptions

a) Thermal-hydraulic data

The thermal-hydraulic data is derived from the calculation results of LB-LOCA scenarios, including pressure, temperature, concentration of CO_2, N_2, O_2, and dose rate etc.

b) Initial concentration

H_3BO_3 and LiOH are assumed to release to IRWST sump at the beginning.

c) The dissolution of TSP

The mass of TSP is 5.62 t in the adjustment basket. The dissolution rate of TSP is 3.42 $kg/m^2 \cdot min$ and the dissolution area is 18 m^2. Therefore, the required time of complete dissolution is 1.52 hours.

After the core outlet temperature exceeds 650 °C, the core is damaged and severe accident mitigation measures need to be launched. The cavity is flooded by large-flow passive injection of EHR [CHRS] in approximately 30 minutes. Then passive injection is switched to small-flow mode. The passive injection water overflows from cavity and is collected by IRWST. The TSP adjustment basket is submerged on the flow path and the dissolution of TSP begins.

13.5.7.2.3 pH Results

The initial pH value of IRWST sump is approximately 5.7. Before the dissolution of TSP, due to the formation of HNO_3, the pH value decreases to near 3.5. After passive injection water overflows from cavity and the dissolution of TSP, the pH value increases to around 7.7. And the pH value of IRWST stays above 7 after the complete dissolution of TSP.

To be conservative, in the modelling of source terms analysis, the pH of IRWST is set at 3.5 in the first 8 hours. After 8 hours, the pH of IRWST is set at 7.

13.5.7.3 Source Terms Assessment

13.5.7.3.1 LB-LOCA

The initial conditions for LB-LOCA are as follows:

a) The initial operation condition is at full power.

b) Double ended rupture of LB-LOCA in the cold leg.

The assumptions for LB-LOCA are as follows:

a) ASG [EFWS] unavailable.

b) Accumulators available.

c) MHSI unavailable.

d) LHSI unavailable.

e) SADV available.

f) EHR [CHRS]available.

g) Passive injection of EHR [CHRS] available.

h) Active injection of EHR [CHRS] available.

i) EUH [CCGCS] available.

j) EDE [AVS] available.

k) DWL [SBCAVS] available.

The operator actions for LB-LOCA are as follows:

a) Passive injection of EHR [CHRS] is delayed by 20 minutes after core outlet temperature exceeds 650°C.

b) Active injection of EHR [CHRS] is activated when the IVR tank is empty.

c) Containment spray of EHR [CHRS] is started 12 hours after core outlet temperature exceeds 650°C.

13.5.7.3.2 LOOP

The initial conditions for LOOP are as follows:

a) The initial operation condition is at full power.

b) Loss of offsite power.

The assumptions for LOOP are as follows:

a) EDG unavailable.

b) SBO diesel generator unavailable.

c) ASG [EFWS] unavailable.

d) Accumulators available.

e) MHSI unavailable.

f) LHSI unavailable.

g) SADV available.

h) EHR [CHRS] available.

i) Passive injection of EHR [CHRS] available.

j) Active injection of EHR [CHRS] available.

k) EUH [CCGCS] available.

l) EDE [AVS] available.

m) DWL [SBCAVS] unavailable in the first 12 hours and available after the first 12 hours.

The operator actions for LOOP are as follows:

a) SADV is opened when core outlet temperature exceeds 650°C.

b) Passive injection of EHR [CHRS] is delayed by 20 minutes after core outlet temperature exceeds 650°C.

c) Active injection of EHR [CHRS] is activated when the IVR tank is empty.

d) Containment spray of EHR [CHRS] is started 12 hours after core outlet temperature exceeds 650°C.

13.5.7.4 Source Terms Results

The detailed information of analysis method and calculation results are presented in the severe accident source terms analysis report [81]. The release time, fractions and radioactivity of nuclides are given.

13.5.8 Practically Eliminated Situations

With safety features and accident management, the UK HPR1000 successfully reduces the risk of an early or large radioactive release to the environment to an acceptable level [82].

13.5.8.1 Methodology of Practical Elimination Demonstration

An early or large radioactive release caused by accident sequences or phenomena which is assumed if one of the containment failure modes occurs has been practically eliminated:

a) If it is physically impossible for the accident sequence or phenomena to occur, or

b) If the accident sequence can be considered with a high degree of confidence to be extremely unlikely to arise.

'Physically impossible' means that certain features make the further development of the accidents impossible.

'Extremely unlikely with a high degree of confidence' means:

a) Total frequency of an early or large radioactive release shall be lower than 10^{-6} per reactor year.

b) The frequency of each release category shall be lower than 10^{-7} per reactor year.

c) The RPTs defined in the General Safety Requirements [41] should be satisfied.

The process of practical elimination demonstration is shown in Figure F-13.5-14 and there are five main steps in this demonstration.

Step 1 is the identification of accident sequences or phenomena which may lead to early or large radioactive release. The source of an early or large radioactive release includes the reactor core and the spent fuel pool. For release from the spent fuel pool, an early or large radioactive release caused by the accident of spent fuel failure should be practically eliminated. For release from the reactor core, according to different containment failure modes, there are four release paths after severe accidents:

a) Release path from containment isolation failure.

b) Release path from containment rupture.

c) Release path from containment bypass.

d) Release path from base melt through.

Besides the above containment failure modes, the containment may be open before the accident. If severe accidents happen during this situation, large volumes of radioactive nuclides may be released out of the containment. This condition must also be demonstrated as practically eliminated.

In the UK HPR1000, the following accident sequences or phenomena may lead to early or large radioactive release:

a) MCCI.

b) DCH.

c) Hydrogen combustion and explosion.

d) Steam explosion.

e) Containment overpressure.

f) Rupture of a Large Component in the Reactor Coolant System.

g) Large reactivity insertion.

h) Containment isolation failure.

i) Containment bypass.

j) Severe accidents with an open containment.

k) Fuel failure in the spent fuel pool.

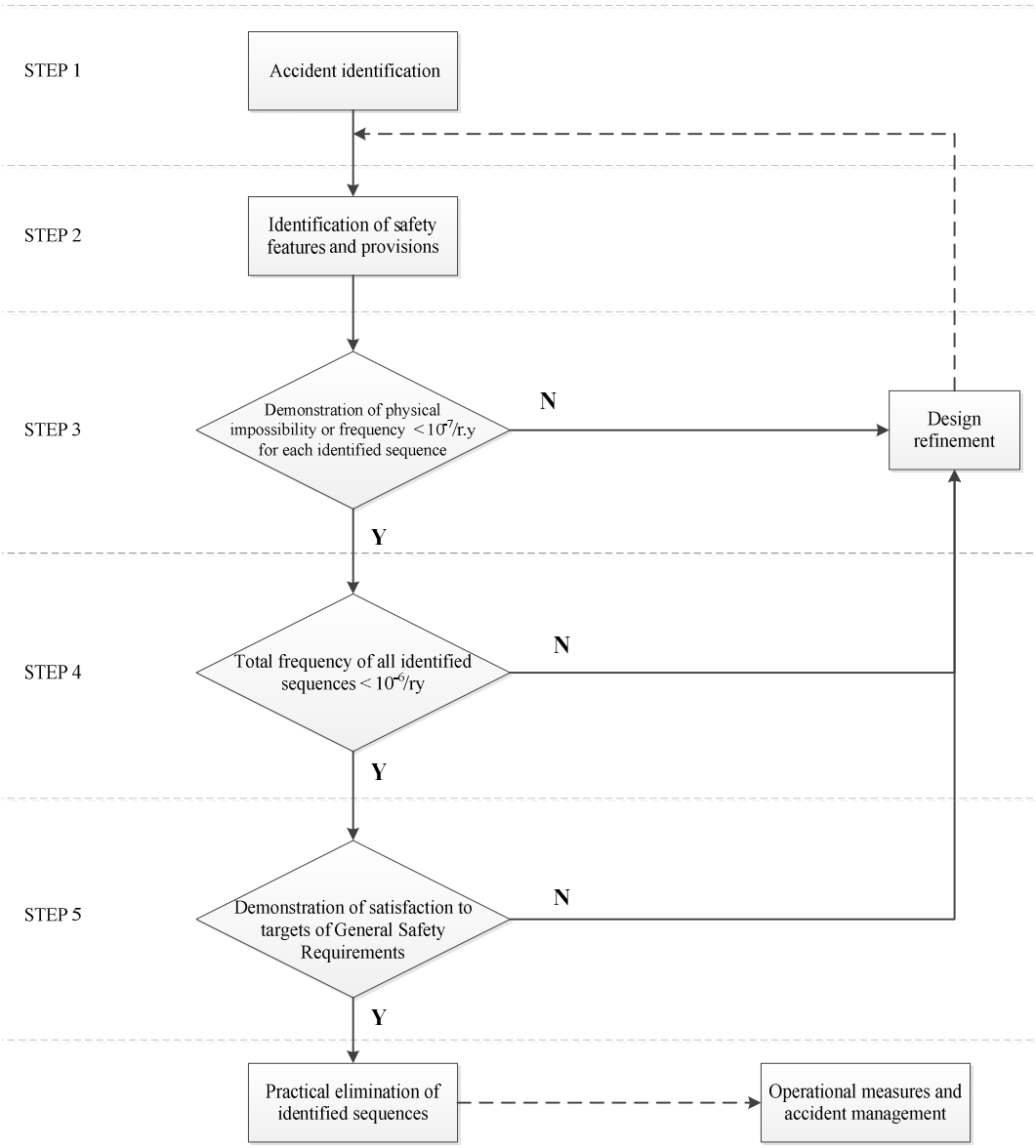
Step 2 is the description of additional reasonably practicable design features, dedicated engineered safety features, operational measures or accident management procedures of each identified accident sequence or phenomenon to lower the risk of an early or large radioactive release on the concept of defence in depth.

Step 3 is the demonstration of practical elimination of early or large radioactive releases caused by each identified accident sequence or phenomenon via 'physically impossible' or 'extremely unlikely'. If early or large radioactive release cannot be demonstrated to be practically eliminated, design refinements will be considered.

Step 4 is the demonstration that the total frequency of identified accident sequences or phenomena is lower than 1.0E-06 per reactor year if each identified accident sequence or phenomenon is demonstrated.

Step 5 is the assessment of radiological consequence of identified accident sequences or phenomena and the demonstration of satisfaction for the targets defined in the General Safety Requirements [41]. In this step, Level 3 PSA results will be used.

Practical elimination is demonstrated after the five steps below in F-13.5-14. However, the practical elimination should not be analysed, only based on a cut-off probabilistic value. If it is possible to lower the risk or the consequence of the accident sequences or phenomena, any additional operational or accidental management measures are supposed to be implemented.



F-13.5-14 Flow-chart of Practical Elimination

13.5.8.2 Practical Elimination Demonstration

13.5.8.2.1 Direct Containment Heating

Diverse systems are designed for the UK HPR1000 to prevent the reactor core from melting in case of different initiating events. If all the prevention measures fail and core melting occurs, SADVs are designed to convert high pressure core melting sequences into low pressure sequences with a high reliability so that high pressure core melting situations can be ‘practically eliminated’.

According to the deterministic analysis and the probabilistic analysis, the frequency of an early or large release caused by DCH is lower than 1.0E-07/ry which corresponds to practical elimination.

13.5.8.2.2 Hydrogen Combustion and Explosion

Diverse systems are designed for the UK HPR1000 to prevent the reactor core from melting in case of different initiating events. If all the prevention measures fail and core melting occurs, the EUH [CCGCS] is designed and facilitated in the containment to mitigate the hydrogen risk.

According to the deterministic analysis and the probabilistic analysis, the frequency of an early or large release caused by hydrogen combustion and explosion is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.3 Containment Failure Caused by Steam Explosion

Diverse systems are designed for UK HPR1000 to prevent the reactor core from melting in case of different initiating events. According to international research, the failure of the containment by an in-vessel steam explosion is highly unlikely. If all the prevention measures failed and the core melting occurs, IVR is designed to keep the integrity of RPV and prevent the ex-vessel steam explosion.

According to the deterministic analysis and the probabilistic analysis, the frequency of an early or large release caused by containment failure caused by steam explosion is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.4 MCCI

Diverse systems are designed for UK HPR1000 to prevent the reactor core from melting in case of different initiating events. If all the prevention measures failed and the core melting occurs, IVR is designed to keep the integrity of RPV and prevent MCCI.

According to the deterministic analysis and the probabilistic analysis, the frequency of an early or large release caused by MCCI is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.5 Containment Overpressure

Diverse systems are designed for UK HPR1000 to prevent the reactor core from melting in case of different initiating events. If all the prevention measures failed and the core melting occurs, EHR [CHRS] and EUF [CFES] are designed to prevent containment overpressure.

According to the deterministic analysis and the probabilistic analysis, the frequency of an early or large release caused by MCCI is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.6 Rupture of a Large Component in the RCP [RCS]

The structural integrity class of the RPV, the PZR and the steam generator are all High Integrity Components (HIC) of the UK HPR1000. The safety objectives are to ensure

the high integrity reliability of the main components to meet their safety functions.

According to HIC analysis and the probabilistic analysis, the frequency of an early or large release caused by rupture of major pressure retaining components is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.7 Large Reactivity Insertion

The negative feedback to reactivity is designed in the UK HPR1000 to avoid the positive reactivity insertion and the power rise. Despite the inherently safe characteristics of the UK HPR1000 reactor core, various prevention measures are designed for the scenario of homogeneous and heterogeneous boron dilution.

According to the deterministic and probabilistic analysis, the frequency of an early or large release caused by large reactivity insertion is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.8 Containment Isolation Failure

Diverse systems are designed for UK HPR1000 to prevent the reactor core from melting in case of different initiating events. In order to ensure the containment isolation function, Containment Isolation and Containment Leak Rate Testing and Monitoring System (EPP [CLRTMS]) are designed in UK HPR1000.

According to the deterministic and probabilistic analysis, containment isolation and EPP [CLRTMS] can achieve the confinement of radioactivity. The frequency of an early or large radioactive release due to the containment isolation failure is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.9 Containment Bypass

Diverse systems are designed for UK HPR1000 to prevent the reactor core from melting in case of different initiating events. An early or large radioactive release due to the containment bypass can be avoided by the reliable design of SG and containment isolation and EPP [CLRTMS].

According to the deterministic of SGTR and ISLOCA and probabilistic analysis, the frequency of an early or large radioactive release due to the containment bypass is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.10 Severe Accidents with an Open Containment

The airlocks and the hatch are allowed to be opened in special plant operation modes due to maintenance. The design of double-seals and double-channel interlocking doors ensure the opening of the personnel airlock and emergency personnel airlock will not lead to loss of containment sealing. For the hatch, it can be closed when the equipment transportation is finished or an initiating event occurs.

According to the above deterministic and probabilistic analysis, severe accidents in an

open containment in RCD mode or due to the opening of the airlock is practical elimination physically, while the frequency of an early or large radioactive release caused by a severe accident in open containment due to the opening of the equipment hatch in all the operation modes except RCD mode is lower than 1.0E-07/ry which means practical elimination.

13.5.8.2.11 Fuel Failure in Spent Fuel Pool

The PTR [FPCTS], ASP [SPHRS] water tank or external emergency makeup source, Reactor Boron and Water Makeup System (REA [RBWMS]) and NI Demineralised Water Distribution System (SED [DWDS (NI)]) are designed to remove the decay heat of the fuel assemblies stored in the SFP in normal and accident conditions (DBC-1/2/3/4 and DEC-A) by cooling the SFP and maintained the SFP water level to cover spent fuels in the SFP by water makeup.

According to the deterministic analysis of SFP and PSA analysis, the frequency of an early large release or early release caused by fuel failure in SFP is lower than 1.0E-07/ry which means practical elimination.

13.5.8.3 Conclusion

The demonstration of practical elimination of the UK HPR1000 is based on the safety design, accident management, PSA, accident analysis, and radiological consequence assessment with consideration of the diverse and redundant mitigation measures and the concept of defence in depth.

The demonstration of satisfaction of targets defined in General Safety Requirements [41], and the assessment of pressure loads induced by slow deflagration or flame acceleration and the frequency analysis of heterogeneous dilution will be added in Step 4. If the total frequency is lower than 10^{-6} per reactor year and the radiological consequence assessment satisfies the targets defined in General Safety Requirements [41], it can be concluded that the accident sequences or phenomena with an early or large radioactive release can be considered practically eliminated.

13.5.9 Severe Accident Environmental Conditions

In the UK HPR1000, the EHR [CHRS] and EUF [CFES] have significant influence on the containment temperature and pressure under severe accidents. The EHR [CHRS] is designed for long-term containment heat removal and containment pressure control under severe accidents. The EUF [CEFS] is an alternative and ultimate way to mitigate the risk of containment overpressure while the containment spray of EHR [CHRS] is failure. So the sensitivity analysis on the availability of EHR [CHRS] and EUF [CFES] should be considered as follows:

a) EHR [CHRS] available.

b) Active functions of EHR [CHRS] unavailable.

13.5.9.1 Accident sequences analysis

According to Reference [45], the accident scenarios selected for severe accident mitigation measures assessment are bounding sequences. They cover different severe accident phenomena and different mass and energy release rates from RCP [RCS] to containment. Therefore, the severe accident scenarios for the analysis of severe accident environmental conditions will be selected based on the accident list which is used for the severe accident mitigation measures assessment.

a) EHR [CHRS] available

LB-LOCA, SB-LOCA, SBO and ATWS sequences are selected for the severe accident environmental conditions analysis based on deterministic and engineering judgements. These scenarios cover severe accident sequences with respect to timing (fast, intermediate, slow scenarios). Considering that the accident progression of IB-LOCA can be covered by LB-LOCA and SB-LOCA, it is not be analysed.

b) Active functions of EHR [CHRS] unavailable

According to the system function of EUF [CFES], it is designed to mitigate the containment overpressure risks caused by long term loss of all AC power scenarios like Fukushima accident. So loss of all AC power is considered as initiating event. LB-LOCA in the hot leg is also assumed as an initial accident at the same time, in which there is a rapid containment pressure increase resulting in higher risk of containment overpressure. Therefore, the LB-LOCA with loss of all AC power is conservative scenario and is selected to determine the severe accident environmental condition under the situation that EUF [CFES] opens.

ASTEC is used to calculate these accident sequences which are selected for severe accident environmental conditions determination.

13.5.9.2 Results

According to the calculation results of these scenarios, the bounding curves that cover the results of all scenarios are determined. Meanwhile, the peak pressure generated by hydrogen combustion is considered in the final environmental conditions. The detailed analyses are shown in the supporting documents [83].

13.5.10 Basic Strategy of SAMG

The SAMG and Emergency Operating Procedure (EOP) are different procedures to deal with accidents in Nuclear Power Plants (NPPs). While the EOP focuses on protecting core integrity, the SAMG pays attention to ensuring containment integrity and limiting the release of fission products to the environment. The SAMG, whose general objective is to reach a controlled and stable state, should cover all the DEC-B scenarios using realistic assumptions. Furthermore, the equipment required for severe accident mitigation should be qualified for the conditions and the necessary mission

time.

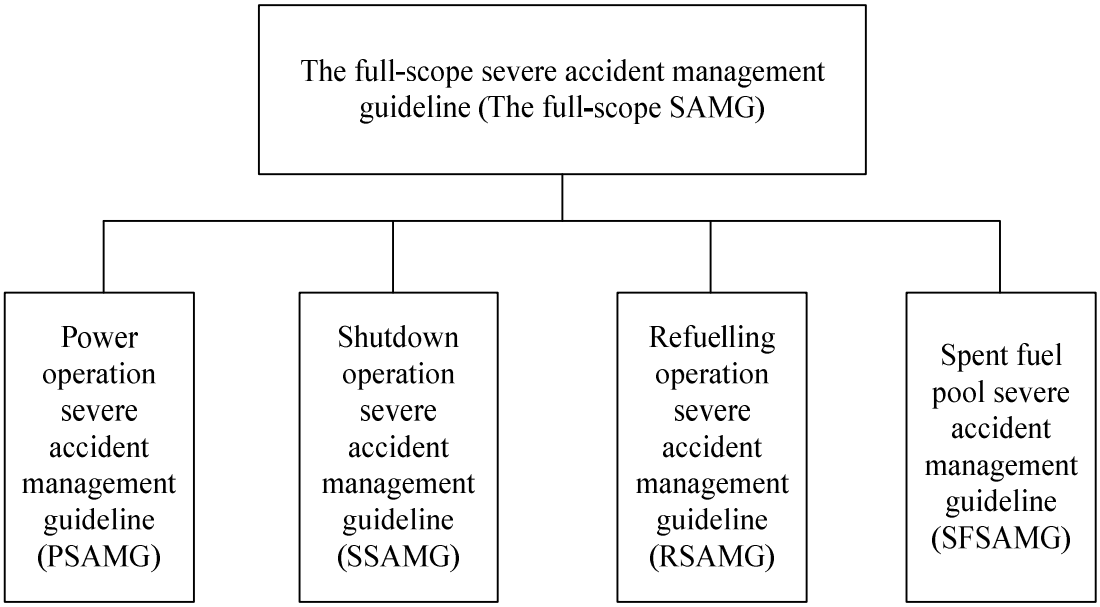
The transition from the EOP to SAMG is based on the core outlet temperature and/or dose rate in the containment (water level and/or dose rate in the SFP). These criteria are continuously monitored whilst the EOP is in progress. When the entry criterion is reached, the SAMG is used instead of the EOP. The decision of using the SAMG is made by an appropriate person according to the requirements in the UK (e.g. the Emergency Controller).

The SAMG is an integrated document for a nuclear power plant to deal with severe accidents effectively. The requirements of the 'Safety Assessment Principles for Nuclear Facilities', Reference [42], prescribe that "Accident management strategies should be developed to manage the escalation of accidents and to restore control"; and "Where the hazard potential is significant, the Hazard Identification and Risk Evaluation (HIRE) should be informed by severe accident analysis. The strategies should aim primarily to prevent the breach of barriers to release or, where this cannot be achieved, to mitigate accident consequences. Their ultimate aim should be to return the facility and/or site to a stable, safe state." The rule on 'Severe Accident Management Programmes for Nuclear Power Plants' prescribes that "In view of the uncertainties involved in severe accidents, severe accident management guidance should be developed for all physically identifiable challenge mechanisms for which the development of severe accident management guidance is feasible; severe accident management guidance should be developed irrespective of predicted frequencies of occurrence of the challenge", Reference [84].

For severe accidents, the design must consider the overall design capacity of the nuclear power plant, including using certain systems (safety and non-safety systems) beyond their predefined functions or in unanticipated operation states and using additional temporary systems, in order to enable the nuclear power plant to return to a controlled and stable state and mitigate the consequences of severe accidents. Subsequently, full-scope SAMG research will be carried out in the site specific assessment stage.

13.5.10.1 Framework of Full-scope SAMG

The full-scope SAMG is an advanced SAMG which deals with severe accidents occurring during all different operation modes of the UK HPR1000 nuclear power plant, containing the power operation mode, shutdown operation mode, refuelling operation mode and severe accidents occurring in the spent fuel pool. A simple framework of the full-scope SAMG is shown in Figure F-13.5-15 [85].



F-13.5-15 Framework of the full-scope SAMG

13.5.10.2 Framework of a Single SAMG

The SAMG highlights three actions which shall be taken by staff of the MCR and Technical Support Centre (TSC) during severe accidents: (1) prevent further deterioration of the core if the core has been damaged and ensure melt retention in the RPV; (2) maintain the containment integrity as long as possible; and (3) minimise offsite release. If divided according to the persons in charge, the SAMG includes the sections used by the MCR and TSC, respectively.

The section used by the MCR includes initial response guidelines which specify actions without assessing the negative and positive effects. The main actions adopted in these guidelines are still the main strategy in the EOP (for example, the injection-discharge strategy of the main system) or instructions given by the TSC (once the TSC is in charge). Meanwhile, some significant parameters will be monitored in the MCR.

The section used by the TSC includes severe accident diagnosis flow charts and mitigation guidelines. As the main part of the SAMG, the most important parameters will be chosen to help the TSC to decide which mitigation strategies should be implemented according to the parameters. Typical calculation aids will be given in advance, which can greatly improve the analysis and judgment abilities of the TSC technicians.

Long-term monitoring and exit guidelines used by the TSC are also considered in the SAMG, which helps to: (1) supervise whether the taken measures are implemented consistently, (2) assess possible recovery actions, and (3) evaluate whether equipment with restored functions is required to be put into operation. The purpose of these guidelines is to provide a tool for the TSC to identify the plant status and confirm and

assess whether the nuclear power plant has returned to a non-emergency state after the strategies and actions in the SAMG have been implemented. Long term concerns associated with the exiting SAMG include core state, method of heat removal, containment state, effectiveness of mitigation strategies and offsite release controlling strategies, and whether failed systems have been restored or not [86].

13.5.11 Lessons Learnt from Fukushima Accident

On March 11, 2011, a magnitude 9 earthquake occurred at the Fukushima Daiichi site in Japan. Then inundation of the plant site by the tsunami wave resulted in loss of electrical supplies and cooling systems, which caused severe core damage to the operating reactors resulting in a large radioactive release to the environment.

In the design of the HPR1000 (FCG3), the lessons learnt from the Fukushima accident have been taken into account, and a number of design modifications have been implemented.

The UK HPR1000 takes the HPR1000 (FCG3) as the reference design, and lessons from Fukushima accident are also addressed in the design of the UK HPR1000, which can be summarised in the following five aspects:

a) Protection design against external hazards (earthquake, flooding)

   The design of the UK HPR1000 ensures the safety objectives of the plant under design basis external hazards, provides margin for beyond design basis external hazards and ensures there are no cliff-edge effects.

b) Dealing with design extension conditions: loss of AC power and cooling chain

   The extreme plant conditions in the Fukushima accident can be defined as loss of AC power and cooling chain. In the UK HPR1000, station black out diesel generators, EHR [CHRS] and ECS [ECS] are designed to ensure emergency power supply and residual heat removal under extreme plant conditions like those experienced in the Fukushima accident.

c) Severe accident management

   The objective of severe accident management is to maintain as many barriers between the core and the environment as possible for as long as possible, even if under extreme plant conditions like those experienced in the Fukushima accident. Strategy of Primary Depressurisation, IVR, Hydrogen Control, Containment Heat Removal and others related to minimising the release of activity to the environment in severe accidents are considered in the UK HPR1000.

d) Emergency preparedness in design

   Emergency response facilities are designed to coordinate and manage site actions under normal and emergency conditions, which mainly include Main Control

Room, Remote Shutdown Station, On-site Emergency Control Centre, Technical Support Centre and Operation Support Centre.

e) Nuclear safety culture and emergency organisation

Release policy statements and procedures to ensure that all personnel participating in the project have a comprehensive understanding of nuclear safety. Establish an organisational culture of transparency, cooperation and communication, and necessary incentive mechanism. Continuously promote a positive safety culture, such as periodic awareness training, performing special activities to improve procedure quality and human behaviours.

Detailed information about lessons learned from Fukushima accident is showed in *Lessons Learned from Fukushima*, Reference [87].

13.6 ALARP Assessment

13.6.1 Scope of ALARP

According to the Reference [88], the DEC-A analysis plays the following roles in the ALARP demonstration of the UK HPR1000 design:

a) DEC-A analysis which support diverse protection lines is provided and demonstrated to be effective for frequent faults.

b) DEC-A analysis which does not support diverse protection lines is provided to demonstrate the effectiveness of defence in depth measures.

In this section, ALARP assessment on severe accident analysis is presented.

According to the 2014 SAPs, SAA should consider questions like ‘what more can reasonably be done?’ or ‘what would need to be done in such an event?’ ALARP evaluation needs to be performed to ensure that the risk to the UK HPR1000 from severe accidents is ALARP [59]. The relevant good practices are the starting point of the ALARP evaluation of the UK HPR1000. As the reference design of the UK HPR1000, the HPR1000 (FCG3) has incorporated international good practice in severe accident mitigation measures, such as: in-vessel corium retention, primary depressurisation valve, hydrogen recombiners, active containment heat removal and containment venting. The HPR1000 (FCG3) is an evolutionary design having progressively reduced risks as the design developed. These engineered severe accident mitigation measures and the overall severe accident strategy are part of this evolution.

The purpose of the SAA ALARP assessment is to demonstrate that there are no further reasonably practical improvements within any of the individual severe accident mitigation measures or for the accident management strategy as far as implementing these measures is concerned that would further reduce risks. Or, if any such potential improvements can be identified, to then assess them further to determine the practicality of their implementation and then incorporate in to the design if it is

reasonably practicable.

Severe accident phenomena and mitigation strategy are the main concern of ALARP assessment of the SAA area. Severe accident mitigation measures are determined based on the overall methodology of SAA and the effectiveness of each system is assessed to demonstrate that the risk of corresponding severe accident phenomena is reduced.

The scope will consider the reactor, spent fuel pool and any other sources of severe accidents if identified.

The scope will not include an assessment of flexible equipment stored off-site; such an assessment would be difficult given that factors affecting the performance such as time to deployment will depend on the site location. Use of such equipment is not precluded by the design since connection points for such equipment will be provided. The future licensee may therefore consider these measures as part of the ALARP assessment for site licensing.

The ALARP evaluation will be performed throughout the GDA process. The approach and main process are described below.

13.6.2 Holistic ALARP Assessment

The design of SA mitigation measures in HPR1000 is not established from zero. The development process of the HPR1000 (FCG3) was based on relevant good international practice demonstrating a continuous improvement of safety performance. Previous experience of CGN on design, modification, and analysis forms a good basis of the present design. The latest international research specific to severe accidents, , innovative and well proven technology, Relevant Good Practice (RGP), and feedback from Fukushima accident are taken into consideration during the modification of existing plants and design of new reactors in CGN.

The ALARP principle requires all measures be taken to reduce risk where doing so is reasonable. As indicated in NS-TAST-GD-007 and ONR-GDA-GD-007, cost-benefit analysis may not be a proper way to determine severe accident mitigation measures, and meeting the standard of relevant good practice will be synonymous with achieving ALARP in many cases. The documents generated by international authorities and organisations, and practice in previous GDA projects can form a good basis of RGP.

System design and detailed analysis are performed to make sure that the design targets of each system are met and the risks induced by severe accident phenomena are ALARP. Based on the analysis results in PCSR Chapter 13.5, the severe accident mitigation measures are demonstrated to avoid severe accident phenomena that could threaten the containment integrity with enough margin in system capacity and operation time. No significant risk is identified based on present studies.

The risk of flame acceleration will be further analysed in 2020 to confirm that pressure load induced by potential hydrogen combustion will not challenge the integrity of containment with presence of EUH [CCGCS].

For the analysis of IVR, EUH [CCGCS], and severe accident source term, uncertainties present in key models and parameters that affect the analysis results. Sensitivity studies on these aspects are planned to cover this in 2020. This work is to demonstrate that the conclusions in SAA area are robust.

For EUF [CFES], the system justification involving several technical areas is ongoing and will be accomplished in 2020.

13.7 Concluding Remarks

Chapter 13 presents the following aspects of design extension conditions of the UK HPR1000:

Safety objectives of DEC-A sequences and DEC-B events are introduced to show how the UK HPR1000 design will meet the general safety requirements.

A set of codes and standards that reflect the latest understanding on design extension conditions are identified. The methodologies of DEC-A and DEC-B analysis are based on this effort.

The DEC-A sequence list is identified. Detailed analysis of identified DEC-A sequences are performed to demonstrate that the faults just beyond DBC can be protected by DEC-A features. Thus, the cliff edge effects beyond design basis are proven to be eliminated.

With probabilistic and deterministic methods combined with engineering judgements, DEC-B sequences are selected to perform the severe accident mitigation measures assessment. With detailed analysis, it is proven that the SA mitigation measures are effective to control the event progression and minimise the radiological consequences after core melt. The risk of a large or early radioactive release is proven to be practically eliminated based on the DEC-B analysis results. Lessons learnt from Fukushima are introduced to show how they are considered in the UK HPR1000 design.

It should be noted that design changes made during Step 3 have not been totally reflected in the present version of DEC-A and Severe Accident analysis reports due to the design development progress of the UK HPR1000. The relevant safety assessment reports of DEC-A and Severe Accident will be updated based on the latest version of the UK HPR1000 design reference.

13.8 References

[1] CGN, UK HPR1000 Design Reference Report, NE15BW-X-GL-0000-000047,

Rev. D, 2019.

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

[3] CGN, Suitability Analysis of Codes and Standards in Severe Accident Analysis, GHX00800009DRAF02GN, Rev. A, 2019.

[4] CGN, Methodology of DEC-A Identification, GHX00100068DOZJ03GN, Rev. A, 2018.

[5] CGN, Identification of DEC-A Sequences, GHX00600001DOZJ02GN, Rev. B, 2019.

[6] CGN, The Design Condition List and Acceptance Criteria, GHX00100029DOZJ04GN, Rev. G, 2019.

[7] CGN, Methodology of DEC-A Analysis, GHX00600175DRAF02GN, Rev. B, 2018.

[8] CGN, NSSS Operating Parameters, GHX00100003DRRG03GN, Rev. D, 2019.

[9] CGN, Total Loss of Feedwater (State A), GHX00600074DRAF02GN, Rev. D, 2019.

[10] CGN, Small Break - Loss of Coolant Accident (SB-LOCA) with Failure of Medium Pressure Rapid Cooldown (MCD) (State A), GHX00600096DRAF02GN, Rev. D, 2019.

[11] CGN, SB-LOCA with Total Loss of Low Head Safety Injection (LHSI) (State A), GHX00600098DRAF02GN, Rev. C, 2019.

[12] CGN, Small Break - Loss of Coolant Accident (State C\D\E), GHX00600001DRAF02GN, Rev. C, 2019.

[13] CGN, Total Loss of Cooling Chain in Shutdown Condition, GHX00600120DRAF02GN, Rev. C, 2019.

[14] CGN, Station Black Out (SBO) (State A), GHX00600025DRAF02GN, Rev. C, 2019.

[15] CGN, Station Black Out (SBO) for Spent Fuel Pool (State A to F), GHX00600117DRAF02GN, Rev. D, 2019.

[16] CGN, Station Black Out (SBO) in Shutdown Condition, GHX00600026DRAF02GN, Rev. C, 2019.

[17] CGN, Functional Requirements of the KDS [DAS], GHX00600248DRAF02GN, Rev. B, 2019.

[18] CGN, DNBR Design Limit, GHX00100001DRRG03GN, Rev. F, 2019.

[19] CGN, Anticipated Transient Without Scram (ATWS) Due to Protection System (RPS [PS]) Failure (State A), GHX00600300DRAF02GN, Rev. A, 2019.

[20] CGN, ATWS by Rods Failure - Loss of Main Feedwater (State A), GHX00600078DRAF02GN, Rev. C, 2019.

[21] CGN, ATWS by Rods Failure - Loss of Offsite Power (State A), GHX00600031DRAF02GN, Rev. C, 2019.

[22] CGN, ATWS by Rods Failure - Small Break - Loss of Coolant Accident (SB-LOCA) (State A), GHX00600286DRAF02GN, Rev. B, 2019.

[23] CGN, ATWS by Rods Failure - Spurious Pressuriser Spraying (State A), GHX00600287DRAF02GN, Rev. B, 2019.

[24] CGN, ATWS by Rods Failure - Excessive Increase in Secondary Steam Flow (State A), GHX00600301DRAF02GN, Rev. A, 2019.

[25] CGN, ATWS by Rods Failure-Steam Line Break in Downstream of Main Steam Isolation Valve (MSIV) (State A), GHX00600302DRAF02GN, Rev. A, 2019.

[26] CGN, Small Break - Loss of Coolant Accident (SB-LOCA) with Total Loss of Medium Head Safety Injection (MHSI) (State A), GHX00600097DRAF02GN, Rev. D, 2019.

[27] CGN, Total Loss of Cooling Chain (TLOCC) with Reactor Coolant Pump Sealing Leakage (State A), GHX00600119DRAF02GN, Rev. C, 2019.

[28] CGN, Loss of Three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) Trains, GHX00600250DRAF02GN, Rev. B, 2019.

[29] CGN, Loss of Ultimate Heat Sink (LUHS) for 100 hours (states A and B), GHX00600251DRAF02GN, Rev. B, 2019.

[30] CGN, Uncontrolled primary water level drop without Safety Injection (SI) signal from Protection System (RPS [PS]) (States C3b and D), GHX00600206DRAF02GN, Rev. B, 2019.

[31] CGN, Multiple Steam Generator (SG) tubes rupture (10 tubes) (State A), GHX00600086DRAF02GN, Rev. C, 2019.

[32] CGN, Main Steam Line Break (MSLB) with Steam Generator Tube Rupture (SGTR) (1 tube) in the affected SG (State A), GHX00600080DRAF02GN, Rev. C, 2019.

[33] CGN, SGTR (1 tube) with Atmospheric Steam Dump System (VDA [ASDS]) stuck open in the affected SG (State A), GHX00600087DRAF02GN, Rev. C,

2019.

[34] CGN, Total Loss of Cooling Chain with Loss of Secondary Cooldown (failure of ASG [EFWS] or VDA [ASDS]) (State A), GHX00600319DRAF02GN, Rev. A, 2019.

[35] CGN, Source Term Analysis of Large Break - Loss of Coolant Accident, GHX00600008DRAF02GN, Rev D, 2019.

[36] CGN, Dropping of Fuel Assembly, GHX00600131DRAF02GN, Rev C, 2019.

[37] CGN, Primary Coolant Source Term Calculation Report, GHX00800006DRDG03GN, Rev C, 2019.

[38] NRC, Iodine Behavior in a PWR Cooling System Following a Postulated Steam Generator Tube Rupture Accident, NUREG-0409, January 1978.

[39] NRC, Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors, RG 1.183, July 2000.

[40] CGN, DEC-A Source Term Analysis, GHX00600009DRAF02GN, Rev. A, 2019.

[41] CGN, General Safety Requirements, GHX00100017DOZJ03GN, Rev. F, 2019.

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

[43] CGN, Safety case Strategy for Severe Accident Analysis, GHX00600177DRAF02GN, Rev. B, 2018.

[44] CGN, Overall methodology of severe accident analysis, GHX00600007DRAF02GN, Rev. B, 2018.

[45] CGN, Selection of Severe Accident Scenarios, GHX00600058DRAF02GN, Rev. D, 2019.

[46] Bal Raj Sehgal, Nuclear Safety in Light Water Reactors: Severe Accident Phenomenology, Academic Press, First edition, 2012.

[47] R. Le Tellier, L. Saas, S. Bajard CEA, Transient stratification modelling of a corium pool in a LWR vessel lower head, Nuclear Engineering and Design 287 (2015) 68-77, 2015.

[48] NEA, High-pressure melt ejection (HPME) and direct containment heat (DCH), State-of-the-Art Report, OCDE/GE(96)194, NEA/CSNI/R(1996)25, 1996.

[49] NEA, In-Vessel and Ex-Vessel Hydrogen Sources, Report NEA/CSNI/R(2001)15, 2001.

[50] NEA, State-of-the-Art report on Molten-Corium-Concrete interaction and

Ex-Vessel Molten-Core Coolability, NEA/CSNI/R(2016)15, 2016.

[51] Nuclear Regulatory Commission. A Reassessment of the Potential for an Alpha-Mode Containment Failure and a Review of the Current Understanding of Broader Fuel-Coolant Interaction Issues, NUREG-1524, 1995.

[52] NEA, OECD research programme on fuel-coolant interaction steam explosion resolution for nuclear applications-Serena Final Report, NEA/CSNI/R(2007)11, 2006.

[53] T. G. Theofanous, et al. Lower Head Integrity Under Steam Explosion Loads, Nuclear Engineering and Design, 189, 7–57, 1999.

[54] D. F. Fletcher. A review of the available information on the triggering stage of a steam explosion. Nuclear safety. Vol. 35, No. 1, January 1994.

[55] I. Huhtiniemi, D. Magallon. Insight into steam explosions with corium melts in KROTOS. Nuclear Engineering and Design 204 (2001) 391–400, 2000.

[56] P. Piluso, G. Trillon, D. Magallon. Material Effect and Steam Explosion at High Temperature (T>2300K), International Journal of Thermophysics, Vol. 26, No. 4, July 2005.

[57] IRSN, Description of the physical models of the premixing application. MC3D code user guide. PSN-RES/SAG/2017-00073, Version3.9, 2017.

[58] D. Magallon, I. Huhtiniemi Corium melt quenching tests at low pressure and subcooled water in FARO. Nuclear Engineering and Design 204 (2001) 369–376, 2000.

[59] CGN, ALARP Demonstration Report for Severe Accident Analysis, GHX00100056KPGB03GN, Rev. A, 2019.

[60] CGN, Lessons Learnt from Fukushima, GHX00100112DOZJ03GN, Rev. A, 2019.

[61] EUR, European Utility Requirements for LWR Nuclear Power Plants - Volume 2 Generic Nuclear Island Requirements: Chapter 1 Safety Requirements, Rev. D, 2012.

[62] CGN, RCP-Reactor Coolant System Design Manual Chapter 3 System Functions and Design Bases, GHX17RCP003DNHX45GN, Rev. B, 2019.

[63] CGN, Methodology of Safety Categorisation and Classification, GHX00100062DOZJ03GN, Rev. B, 2018.

[64] CGN, RCP-Reactor Coolant System Design Manual Chapter 6 System Operation and Maintenance, GHX17RCP006DNHX45GN, Rev. D, 2019.

[65] IAEA, Mitigation of Hydrogen Hazards in Severe Accidents in Nuclear Power Plants, IAEA-TECDOC-1661, 2011

[66] CGN, EHR-Containment Heat Removal System Design Manual Chapter 2 Brief Introduction to the System, GHX17EHR002DNHX45GN, Rev. B, 2019.

[67] CGN, EHR-Containment Heat Removal System Design Manual Chapter 3 System Functions and Design Bases, GHX17EHR003DNHX45GN, Rev. B, 2019.

[68] CGN, Equipment Qualification Methodology, GHX80000003DOZJ03GN, Rev. A, 2019.

[69] CGN, EHR-Containment Heat Removal System Design Manual Chapter 4 System and Component Design, GHX17EHR004DNHX45GN, Rev. B, 2019.

[70] CGN, EHR-Containment Heat Removal System Design Manual Chapter 6 System Operation and Maintenance, GHX17EHR006DNHX45GN, Rev. C, 2019.

[71] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 2 Brief Introduction to the System, GHX17EUF002DNHX45GN, Rev. B, 2018.

[72] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 3 System Functions and Design Bases, GHX17EUF003DNHX45GN, Rev. B, 2019.

[73] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17EUF005DNHX45GN, Rev. B, 2019.

[74] CGN, Depressurization Capacity Analysis of Severe Accident Dedicated Valve, GHX00600055DRAF02GN, Rev. C, 2019.

[75] CGN, Assessment of containment combustible gas control system by lumped parameter method, GHX00600103DRAF02GN, Rev. D, 2019.

[76] CGN, Assessment of EUH [CCGCS] by CFD method, GHX00600298DRAF02GN, Rev. B, 2019.

[77] CGN, The thermal shock analysis of RPV while triggering IVR Condition, GHX00100011DPLX44GN, Rev. A, 2019.

[78] CGN, The Structural Integrity Assessment of RPV on In-Vessel Retention Condition, GHX00100014DPLX44GN, Rev. A, 2019.

[79] CGN, Assessment of EHR [CHRS], GHX00600063DRAF02GN, Rev. D, 2019.

[80] CGN, Assessment of EUF [CFES], GHX00600065DRAF02GN, Rev. D, 2019.

[81] CGN, Severe Accident Source Term Analysis, GHX00600258DRAF02GN, Rev. D, 2019.

[82] CGN, Practically eliminated situations, GHX00600127DRAF02GN, Rev. D, 2019.

[83] CGN, Severe Accident Environmental Conditions, GHX00600299DRAF02GN, Rev. A, 2019.

[84] IAEA, Severe Accident Management Programmes for Nuclear Power Plants, NS-G-2.15, 2009.

[85] CGN, General Study Report for Full-scope SAMG, GHX00600121DRAF02GN, Rev. B, 2018.

[86] CGN, Technical Scheme and Framework Development Report for Full-scope SAMG, GHX00600122DRAF02GN, Rev. B, 2018.

[87] CGN, Lessons Learned from Fukushima, GHX00100112DOZJ03GN, Rev. A, 2019.

[88] CGN, ALARP Demonstration Report of Fault Studies, GHX00100055KPGB03GN, Rev. A, 2019.

Appendix 13A Computer Codes Used in the DEC-A and DEC-B Analysis

In the DEC-A analysis, LOCUST, GINKGO, COCO, LINDEN, and ASTEC are used. The information of LOCUST, GINKGO, COCO, and LINDEN is presented in Appendix 12A of Chapter 12.

In the DEC-B analysis, both integral code and dedicated codes are used. The integral code is ASTEC (Accident Source Term Evaluation Code). Dedicated codes used are GASFLOW, MC3D and MOPOL.

ASTEC

The ASTEC code aims at simulating the behaviour of an entire severe accident sequence in a nuclear water-cooled reactor from the initiating event through the release of radioactive materials out of the containment, including the function of engineered safety systems and procedures of severe accident management.

The ASTEC code has the sufficient validation to cover the main physical phenomena, taking into account for safety systems and procedures, with the user-friendly to easily perform sensitivity analyses. Besides, it is equipped with tools for pre-processing, on-line visualization, and post-processing.

ASTEC progressively became the reference European severe accident integral code for water-cooled reactors through the capitalization of new knowledge acquired in the frame of the Severe Accident Research NETwork of excellence (SARNET) from 2004 to 2013.

The main applications are:

- Source term determination studies.

- Level 2 PSA studies including the determination of uncertainties.

- Accident management studies.

- Physical analyses of experiments to improve the understanding of the phenomenology.

The validation and verification of ASTEC is supported by a large set of international experiments, including most aspects of severe accident phenomenology. The validation matrix mainly includes separate-effect tests or coupled-effect tests, integral applications such as the TMI-2 accident and the integral experiments of the Phébus, FP programme, particularly the application to the Organization for Economic and Cooperation Development (OECD) International Standard Problems (ISP) No.46 on the Phébus FPT1 experiment. Moreover, an independent validation work was initiated at end of 2009 in the particular frame of SARNET network and it has since been intensively continued.

GASFLOW

GASFLOW-MPI is a parallel computational fluid dynamics code (CFD) that solves transient three-dimensional compressible Navier-Stokes equations in Cartesian or Cylindrical coordinates. It has the capabilities of simulating turbulent flow, phase exchange, heat and mass exchange between fluid and structure, radiation heat transfer, chemical kinetics, and aerosols. Furthermore GASFLOW-MPI is also equipped with several features specifically for the containment related problems, for instance, the recombiner and igniter model, the spray model, the water film model etc. All these have made GASFLOW-MPI a state-of-art numerical tool for prediction of hydrogen dispersion, combustion, detonation and mitigation in nuclear reactor containments. The code is well validated with several international benchmarks and widely applied in the nuclear industrial field.

GASFLOW is developed by Karlsruhe Institute of Technology (KIT) and it has been used extensively to perform hydrogen safety analysis of Yangjiang units 3&4, Ningde units 3&4 and Fangchenggang units 3&4, etc.

It is a best-estimate tool for predicting transport, mixing, and combustion of hydrogen and other gases in nuclear reactor containments and other facility buildings.

The code has been validated and verified to confirm its applicability in the thermal-hydraulic study in the containment during severe accidents. Comparisons with both analytical solutions and data were performed for the GASFLOW code. During the development of GASFLOW code, many experiments were modelled and analysed. The computational results are in agreement with the analytical solution or the test data.

MC3D

MC3D is used for the analysis of steam explosion. The code is developed by IRSN, it is a thermal-hydraulic multiphase flow code mainly dedicated to ex-vessel and in-vessel Fuel Coolant Interactions (FCI) studies. It has been built with the fuel coolant interaction calculations in mind. It is able to calculate very different situations and has a rather wide field of potential applications.

It has been used to analyse the risk of steam explosions of Yangjiang units 5&6 and Fangchenggang units 3&4.

The MC3D computer code aims at simulating the interaction between the molten fuel and the coolant in the frame of reactor safety studies. The two main applications of MC3D are PREMELANGE, made for premixing calculations, and EXPLOSION, built for the calculations of steam explosions.

To validate the software, MC3D compared its results with analytical or experimental tests, representing only particular aspects or phenomena appearing during the course of an interaction. MC3D also compared its results with global experiments on reduced

scale reproducing most of the features encountered during a hypothetical FCI in a Pressurised Water Reactor (PWR).

MOPOL

MOPOL (MOlten POoL) is a dedicated code used to carry out the sensitive analysis and effectiveness of IVR. This code is based on two-layer molten pool model. The Monte Carlo sampling method is used to sample the different input parameters which have a great influence on heat transfer in the corium pool. The heat flux transfer from the corium pool to the lower head of the pressure vessel is calculated based on the heat transfer model in the molten pool.

MOPOL is developed by CGN and Shanghai Jiao Tong University in 2010. It has been used to calculate the heat flux of corium pool of Yangjiang units 5&6 and Fangchenggang units 3&4.

MOPOL is used to calculate the heat flux transfer from the corium pool to the lower head of pressure vessel. It can also deal with the uncertain parameters using Monte Carlo sampling method.

The heat transfer models of oxidation and light metal layer are based on molten pool simulation tests.