Revision	Approved by	Number of Pages
000		131
Approval Date	12/11 2018	

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

DISTRIBUTION LIST

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

MODIFICATION RECORD

Revision	Section	Page	Modification
000	ALL	ALL	First Issue

TABLE OF CONTENTS

13.1 List of Abbreviations and Acronyms

AAD	Startup and Shutdown Feedwater System [SSFS]
AC	Alternating Current
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
CHF	Critical Heat Flux
DBC	Design Basis Condition
DBF	Design Basis Flood
DCH	Direct Containment Heating
DDT	Deflagration to Detonation Transition
DEC	Design Extension Condition
DEL	Safety Chilled Water System [SCWS]
DNBR	Departure from Nucleate Boiling Ratio
ECS	Extra Cooling System [ECS]
EDG	Emergency Diesel Generator
EHR	Containment Heat Removal System [CHRS]
EOP	Emergency Operating Procedure
EUF	Containment Filtration and Exhaust System [CFES]
EUH	Containment Combustible Gas Control System [CCGCS]

GCT	Turbine Bypass System [TBS]
GDA	Generic Design Assessment
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
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
IVR	In-Vessel Retention
KDS	Diversity Actuation System [DAS]
KIT	Karlsruhe Institute of Technology
LB-LOCA	Large Break (Loss of Coolant Accident)
LCD	Low Pressure Full Cooldown
LHSI	Low Head Safety Injection
LOOP	Loss of Offsite Power
LUHS	Loss of Ultimate Heat Sink
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
ONR	Office for Nuclear Regulation
PAR	Passive Autocatalytic Recombiner
PCSR	Pre-Construction Safety Report
PDF	Probability Distribution Function
PIE	Postulated Initiating Events
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]
RCV	Chemical and Volume Control System [CVCS]
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RIS	Safety Injection System [SIS]
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RRI	Component Cooling Water System [CCWS]
RT	Reactor Trip
SA	Severe Accident
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]
SFP	Spent Fuel Pool
SERG	Steam Explosion Review Group
SG	Steam Generator
SGa	Affected Steam Generator
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
TLOCC	Total Loss of Cooling Chain
TLOFW	Total Loss of Feedwater
TSC	Technical Support Centre
UHS	Ultimate Heat Sink
UK HPR1000	The UK version of the Hua-long Pressurised Reactor
UPS	Uninterruptible Power Supply
VDA	Atmospheric Steam Dump System [ASDS]
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.

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 design extension conditions in the UK version of the Hua-long Pressurised Reactor (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.*

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

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

Claim 3.4*: The safety assessment shows that the nuclear safety risks are As Low As Reasonably Practicable (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 developed several Sub-claims and a number of relevant arguments and evidence:

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

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

Argument 1.1: The DEC-A sequences and protection systems are identified and equipped to cope with multiple failure events.

Argument 1.2: In the DEC-A analysis, the key initial parameters, main system parameters and time delay consider the conservative assumptions.

Argument 1.3: 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.

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

Argument 2.1: The DEC-A sequences analysis is performed until the DEC-A final state is reached.

Argument 2.2: With DEC-A protection systems, the DEC-A sequences are proved to have enough margin.

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

Argument 3.1: International research to date on severe accident phenomena is reviewed.

Argument 3.2: SAA modelling and severe accident analysis are performed.

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

Argument 4.1: The analysis codes and models are suitably verified and validated based on the current state of knowledge.

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

Argument 5.1: The SADVs could effectively avoid high-pressure core melt during a severe accident.

Argument 5.2: The in-vessel retention strategy could maintain the integrity of reactor vessel after core melt.

Argument 5.3: The EHR [CHRS] system could maintain the temperature and pressure of containment below design basis.

Argument 5.4: The Containment Combustible Gas Control System (EUH [CCGCS]) system could reduce the hydrogen risk to a safety level that would not challenge the integrity of containment.

Argument 5.5: The Containment Filtration and Exhaust System (EUF [CFES]) system could maintain the confinement function of containment and avoid the overpressure failure risk.

Argument 5.6: The other mitigation measures excluding dedicated severe accident mitigation systems are effective.

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

Argument 6.1: System design in UK HPR1000 takes account of the lessons learnt from the Fukushima accident.

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

Argument 7.1: The source term analysis codes and models are suitable.

Argument 7.2: The chemical form, possible release categories, magnitude and timing are identified.

Argument 7.3: The design features of the UK HPR1000 and their functions for radionuclides retention and transport are analysed.

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 as 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 13.4.6 - presents the severe accident mitigation measures coping with

DEC-B events and methodology and results of DEC-B analysis;

f) Sub-chapter 13.6 - presents the ALARP evaluation approach;

g) Sub-chapter 13.7 - shows concluding remarks;

h) Sub-chapter 13.8 –gives the references;

i) Appendix 13A – provides the introduction of 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 the total risks and exposure of public and workers from DEC-A and DEC-B events can meet specified numerical targets. Chapter 13 provides the thermal-hydraulic analysis results and source term

PCSR Chapter	Interface
	input to PSA.
Chapter 15	Chapter 13 provides human-related claims (implied and explicit) in the SAA, which need SQEP HF analysis and/or review. Chapter 15 substantiates the claims on operator actions under DEC-A and severe accident conditions.
Chapter 18	Chapter 18 provides external hazards as an input to identify parts of DEC events considered in Chapter 13.
Chapter 20	The organisational arrangements and quality assurance arrangements set out in Chapter 20 are implemented in the design process of all plant SSCs and production of PCSR 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 input for radiological consequence analysis of DEC events.
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 source term release and radiological consequences for emergency preparedness.
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 to be applied should be selected and reviewed according to the principles in the *General Principles for Application of*

Laws, Regulations, Codes and Standards [1]:

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 refer to the Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) in Sub-chapter 13.4.1.2, as the UK HPR1000 PSA is on-going.

The intention is that this Sub-chapter will be updated once the PSA of the UK HPR1000 has been completed to reflect the sources of data for the DEC-A sequences identification.

13.4.1.1 Requirement and Methodology of DEC-A Sequences Identification

A set of design extension conditions 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 design extension conditions 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 is such that it prevents accident conditions that are not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable.

The process of DEC-A sequence identification will consider the following methods [2]:

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

b) Referring to the result from the PSA analysis;

c) Referring to engineering judgment and operating experience.

13.4.1.2 DEC-A Sequences List

As the identification of Postulated Initiating Events (PIE) for the UK HPR1000 and the Level 1 PSA is still on-going, the DEC-A list in this document version refers to the HPR1000 (FCG3). It is acknowledged that there may some changes based on the result of PIE identification and Level 1 PSA analysis. The DEC-A list for the UK HPR1000 will be completed step by step during the GDA. As the fault schedule is under development, the DEC-A work will form an important foundation for diverse protection against all frequent faults.

For the HPR1000 (FCG3), the above approach has been followed to produce the DEC-A list provided in T-13.4-1 below.

T-13.4-1 DEC-A Sequences Considered in the HPR1000 (FCG3) [3]

No.	Sequences Description
1	Total Loss of Feedwater (TLOFW) (State A)
2	Small Break (Loss of Coolant Accident) (SB-LOCA) with failure of Medium Pressure Rapid Cooldown (MCD) (State A)
3	SB-LOCA with total loss of Low Head Safety Injection (LHSI) (State A)
4	SB-LOCA with total loss of LHSI (State C/D)
5	Loss of Residual Heat Removal (RHR) or failure of recovery of RHR after Loss of Offsite Power (LOOP) accident (State C/D)
6	Station Black Out (SBO) (State A to F)
7	SBO, spent fuel pool (State A to F)
8	Anticipated Transient Without Scram (ATWS) due to Reactor Protection System (RPS) failure (State A)

No.	Sequences Description
9	ATWS due to failure of Rod Cluster Control Assembly (RCCA) to insert (State A)
10	SB-LOCA with total loss of Medium Head Safety Injection (MHSI) (State A)
11	Reactor coolant sealing leakage caused by Total Loss of Cooling Chain (TLOCC) (State A)
12	TLOCC (State D)
13	Loss of three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) trains (State A to F)
14	Loss of Ultimate Heat Sink (LUHS) for 100 hours (states A and B)
15	Uncontrolled primary water level drop without SI signal from Reactor Protection System (RPS) (state D)
16	Multiple SG tubes rupture (10 tubes) (State A)
17	Main Steam Line Break (MSLB) with Steam Generator Tube Rupture (SGTR) (1 tube) in the affected SG (State A)
18	SGTR (1 tube) with Atmospheric Steam Dump System (VDA [ASDS]) stuck open in the SG affected (State A)

Notes:

Events postulated in safety analysis are supposed to occur during normal plant operation. The initiating conditions assumed in safety analyses cover all the possible standard conditions from full power operation to cold shutdown. The definitions of the safety analysis domains 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 events with similar functional characteristics can be protected by the same DEC-A features. The features are introduced as follows.

a) 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 is failed.

In the case of Total Loss of Feed Water (TLOFW), the ASP [SPHRS] can be used to

remove the core residual heat effectively and continually in the long term to avoid the core melt. It will be actuated automatically 60s delay after the "SG level (wide range) low 3" signal and all the feedwater flow rates of Emergency Feedwater System (ASG [EFWS]) are low.

b) Extra Cooling System (ECS [ECS])

The ECS [ECS] is designed to provide extra cooling source for Containment Heat Removal System (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]) or/and Essential Service Water System (SEC [ESWS]).

During TLOCC in state A with RCP 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 Spent Fuel Pool (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 3 hours later after the accident.

c) Containment Heat Removal System (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 LHSIs in state A and state D, and Loss of RHR or failure of recovery of RHR after LOOP accident 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.

d) SBO diesel generators

In the case of SBO during all operation modes, the two SBO diesel generators are assumed to be actuated manually by the operator 30 minutes after the first significant signal (like RT signal) to supply electricity to the necessary safety systems and relevant auxiliary systems. During SBO accident in state A, the 2 trains of ASG [EFWS] and VDA [ASDS] are powered by SBO diesel generators to ensure the heat removal of primary system. For SBO accident in state D, the LHSI and Safety Chilled Water System (DEL [SCWS]) are powered by SBO diesel generators to ensure the inventory of primary system, the EHR [CHRS] and ECS [ECS] are supplied by SBO diesel generators to ensure the heat removal in the long time. For SBO accident in SFP, the PTR [FPTCS] and ECS [ECS] need power supply to ensure the SFP cooling.

e) Diversity Actuation System (KDS [DAS])

The KDS [DAS] is designed to deal with DEC-A events which result from failure of

RPS. During ATWS accident due to signal failure, the diverse RT signals are designed for the reactor trip. For the uncontrolled primary water level drop without SI signal from RPS, the "RCP [RCS] loop level low 1" signal is designed to actuate Safety Injection System (RIS [SIS]).

f) 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.

g) Safety Chilled Water System (DEL [SCWS])

In the case of RRI [CCWS] and/or SEC [ESWS] failure, the Safety Chilled Water System (DEL [SCWS]) can offer diverse cooling chain to cool the LHSI pump motors so as to ensure the normal operation of LHSI pumps. During TLOCC accident 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.

h) 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 accident 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 with failure of ASP [SPHRS], manual feed and bleed operation can also be regarded as an 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 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.

i) Low Pressure Full Cooldown (LCD)

Low Pressure Full Cooldown (LCD) is designed to depressurize 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 depressurize down to the LHSI injection pressure. This function is realized by operators via the stepwise pressure setpoint reduction leading to full opening of all VDA [ASDS].

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 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, single failure and preventive maintenance are not considered during DEC-A analysis [4].

a) Input Parameters

The key initial parameters of steady-state conditions are penalized by considering their uncertainties for DEC-A analysis. A summary of the key parameters is shown in T-13.4-2.

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 event. 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.

The non-permanent equipment, such as mobile power and mobile pump, are 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 Reactor Trip (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 [4].

In addition, the acceptance criteria for DEC-A event 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 [4]:

a) The core and SFP fuel assemblies remains sub-critical;

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

c) Confinement of radioactive material is ensured.

13.4.4 DEC-A Key Inputs

This Sub-chapter summaries the input parameters for the DEC-A analysis. A list of inputs for the UK HPR1000 is provided in T-13.4-2.

T-13.4-2 DEC-A Key Input Parameters [4]

Parameters	Values Considering Uncertainties
Core rated thermal power (MW)	3150×(100%±2%)
Reactor Pressure Vessel (RPV) coolant average temperature (°C)	307.0±2.5 (best estimate value) or 307.0±2.5 (Thermal Hydraulic (T/H) design value)
Reactor loop flowrate (m^3/h) (single loop)	25450 (best estimate value) or 24000 (T/H design value)
Core bypass flowrate (%)	6.5 (T/H design value)
Initial pressuriser pressure (MPa)	15.5±0.25
Pressuriser water level (%)	53.1±7

Parameters	Values Considering Uncertainties
Initial SG level (%Narrow Range (NR))	50±10
Main Feedwater Flow Control System ARE [MFFCS] feedwater temperature (°C)	228±2.5

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. Analyses of representative DEC-A sequences are described in detail in following sections. For the rest of the events, brief descriptions are presented and the detailed analyses are shown in supporting documents.

13.4.5.1 TLOFW (State A)

13.4.5.1.1 Description of the Accident

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, which will lead to a decrease in SG inventory. The TLOFW is an overheating DEC-A accident, the SG may dry up and the core decay heat cannot be removed by the secondary system effectively without utilising any other measures.

When a TLOFW accident happens, the SGs will lose feedwater completely. The secondary pressure increases and the VDA [ASDS] will open as part of overpressure protection. The core decay heat is removed by the consumption of SG water and the continual opening of the VDA [ASDS]. As a result, the water levels of the SGs will constantly decrease. Then, the "SG Level (Narrow Range) Low 1" signal will trigger Reactor Trip (RT) for core protection. After RT, the turbine stops. However this is not enough to take the reactor to the final state.

If there are no any other mitigation measures, the SGs may dry up, and the primary pressure and temperature will increase rapidly. The primary coolant will drain away because of the continual opening of Pressuriser Safety Valves (PSVs), which may lead to the damage of fuel and clad. In the UK HPR1000, the ASP [SPHRS] is the key means of heat removal in the TLOFW condition. With the "SG level (wide range) low 3" signal, the ASP [SPHRS] is triggered to remove the core decay heat. However, as the RCP [RCS] pumps keep working, SG level may decrease gradually, until the level reaches the "SG Level (Wide Range) Low 4" value. With the "SG Level (Wide Range) Low 4" signal, the RCP [RCS] pumps begin to coast down and the SG level stops falling. If the "SG Level (Wide Range) Low 4" value cannot be reached because of the activation of the ASP [SPHRS], the operator will stop the RCP [RCS] pumps

manually 30 minutes after the RT signal.

Finally, the temperature and pressure of RCP [RCS] will decrease continuously by the ASP [SPHRS] and the final state will be reached.

13.4.5.1.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.1.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (1.645σ uncertainties on the “B+C term”) is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of TLOFW accident.

1) The RT is triggered by the “SG level (narrow range) Low 1” signal;

2) The ASP [SPHRS] is triggered by the “SG level (wide range) low 3” signal;

3) The VDA [ASDS] open automatically when the SG pressure reach “SG pressure high 1” to limit the secondary pressure.

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from the Main Control Room is assumed to be performed 30 minutes after the first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal. In the TLOFW accident, the operator stops the RCP [RCS] pumps manually 30 minutes after the RT signal.

13.4.5.1.4 Results

The SG water inventory decreases after the TLOFW accident happens. When the water level decreases to “SG level (wide range) low 3”, the ASP [SPHRS] is triggered. Then the SG water level stops falling after the ASP [SPHRS] starts. The primary coolant flow coast down and the primary temperature rises temporarily after the RCP [RCS] pumps are stopped manually. But with the ASP [SPHRS] removing heat from the primary system, the primary temperature decreases continuously.

13.4.5.1.5 Conclusions

The results show that during the whole process of the TLOFW accident, the core is always covered, the core decay heat can be removed continually by the ASP [SPHRS] system. The acceptance criteria are met [5].

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

13.4.5.2.1 Description of the Accident

In the accident of SB-LOCA combined with loss of MCD, the MCD is assumed to fail because of the failure of GCT [TBS] and VDA [ASDS]. Feed and bleed is applied to mitigate this accident.

The primary break leads to the loss of reactor coolant and results in the decrease of the RCP [RCS] pressure and the PZR water level. The “Pressuriser pressure low 2” signal triggers the RT. After the RT, the turbine trip is triggered and the full load isolation valves of the ARE [MFFCS] are closed automatically. Since the GCT [TBS] and VDA [ASDS] are assumed to be unavailable, the secondary pressure rises and is limited by the Main Steam Safety Valve (MSSV). The SGs are refilled with water by the ARE [MFFCS] through the low load pipeline. 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. The “Pressuriser pressure low 3" signal triggers the SI signal. Because of MCD failure, the MHSI cannot inject into the RCP [RCS] since the RCP [RCS] pressure is higher than the MHSI injection pressure.

The final state is reached through manually opening the PSVs. In this analysis, the final state is defined as reaching the RIS [SIS] connection condition in RHR mode. When the operator opens 3 trains of PSVs for depressurisation, the RCP [RCS] pressure drops sharply. After the RCP [RCS] pressure decreases, the MHSI and LHSI begin to inject borated water from the IRWST into the RCP [RCS]. When the RCP [RCS] pressure is low enough, the RIS accumulators begin to inject water into the RCP [RCS].

13.4.5.2.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.2.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (2σ uncertainties on the “B+C term”) is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of the accident.

1) The RT is triggered by the “Pressuriser pressure low 2” signal;

2) The SI signal is triggered by the “Pressuriser pressure low 3” signal;

3) The RCP [RCS] pumps stops due to the combination of a SI signal and “RCP [RCS] pump ΔP low 1” signal.

4) 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.

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from the Main Control Room is assumed to be performed 30 minutes after the first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal. In the accident, the operator will manually open 3 trains of PSVs 30minutes after the RT signal.

After the above measures are taken, the following final state is achieved:

a) Ensure the sub-criticality of the core (through the automatic RT and limited cooldown operation, the addition of borated water is not necessary);

b) Use the SI and PSVs to ensure decay heat removal;

c) Remain the radioactive release controllable (realised through the above measures).

13.4.5.2.4 Results

The pressure of PZR decreases after the SB-LOCA happens. When the PZR pressure decreases to “Pressuriser pressure low 2”, the reactor trip is triggered. Then the MCD will be triggered by the SI signal. However, due to the GCT [TBS] and VDA [ASDS] failures, the primary cooling and depressurization cannot be performed through MCD. Therefore, after reactor trip, the primary pressure and temperature remain high until the intervention of the operator.

The operator opens the PSVs manually 30 minutes after the RT signal and the primary pressure decreases rapidly. The MHSI and LHSI start to inject borated water into the RCP [RCS], the primary temperature and pressure decrease continuously.

13.4.5.2.5 Conclusions

The results show that the automatic actions of reactor protection systems and operator

actions can take the plant to its final state. The acceptance criteria are met [6].

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

13.4.5.3.1 Description of the Accident

When the SB-LOCA with total loss of LHSI happens, the loss of coolant inventory from the break cannot be compensated by the RCV [CVCS]. The primary pressure decreases, and the "Pressuriser pressure low 2" signal triggers the RT. After the RT, the turbine trip is triggered automatically and the full load pipelines of the ARE [MFFCS] are isolated. The SGs are refilled with water by the ARE [MFFCS] through the low load pipeline. 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. When the PZR pressure reaches "Pressuriser pressure low 3", the SI signal is triggered and the MHSI automatically starts. The RCP [RCS] pumps will stop due to the combination of a SI signal and "RCP [RCS] pump ΔP low 1" signal. In the secondary system, the VDA [ASDS] is used to limit the pressure. At the same time, the SI signal will trigger the MCD automatically. The operator will manually open the VDA to cool down the primary system 30 minutes after the first significant signal (such as RT signal). Two trains of RBS [EBS] will be manually started to avoid re-criticality.

In the early stages of the accident, the primary coolant inventory can be maintained by the MHSI. However, the decay heat cannot be removed from the containment effectively in the long term with the failure of LHSI/RHR, which may cause the IRWST water temperature increase and the cavitation of the MHSI pumps. In this accident, the EHR [CHRS] is used to cool down the IRWST and containment to keep the MHSI available in the long term. The heat removal from the IRWST and containment provided by the EHR [CHRS] in the long term is demonstrated to be effective.

13.4.5.3.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.3.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (2σ uncertainties on the "B+C term") is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of the accident.

1) The RT is triggered by the “Pressuriser pressure low 2” signal;

2) The SI signal is triggered by the “Pressuriser pressure low 3” signal;

3) The MCD is triggered by the SI signal;

4) The RCP [RCS] pumps stops due to the combination of a SI signal and “RCP [RCS] pump ΔP low 1” signal.

5) 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.

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from the Main Control Room is assumed to be performed 30 minutes after first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal.

1) Thirty minutes after the RT signal , the operator will manually actuate two trains of RBS [EBS];

2) Thirty minutes after the RT signal , the operator will manually open the VDA to cool down the primary system.

After the above measures are taken, the following final state is achieved:

a) Ensure the sub-criticality of the core (through the automatic RT and limited cooldown operation);

b) Use the ASG [EFWS] and VDA [ASDS] system to ensure decay heat removal;

c) Remain the radioactive release controllable (realised through the above measures).

13.4.5.3.4 Results

The pressure of PZR decreases after the SB-LOCA happens. When the PZR pressure decreases to “Pressuriser pressure low 2”, the reactor trip is triggered. Then the MCD will be triggered by the SI signal, the MHSI starts to inject water into the RCP [RCS]. 30 minutes after the RT signal, the operator manually cools down the primary system. The EHR [CHRS] is used to cool down the IRWST and containment to keep the MHSI available in the long term.

13.4.5.3.5 Conclusions

The results show that the automatic actions of reactor protection systems and operator

actions can take the plant to its final state. The acceptance criteria are met [7].

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

13.4.5.4.1 Description of the Accident

In SB-LOCA combined with total loss of LHSI accidents in state C or D, the MHSI is used to compensate the primary coolant inventory.

In state C (the reactor coolant pumps are running), the SI signal can be triggered by "Hot leg ΔPsat low 1". In state C (the reactor coolant pumps are at shutdown state) and state D, the SI signal can be triggered by "RCP loop level low 1".

After the MHSI is activated, the coolant inventory can be compensated and decay heat is transferred into IRWST. The EHR [CHRS] is used to cool down the IRWST and remove the decay heat from the containment to reach the final state.

13.4.5.4.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.4.3 Analysis Methods

Qualitative assessment method is used to analyse the process of this accident.

13.4.5.4.4 Results

In state C or state D, the coolant mass flow rate through the break can be bounded by SB-LOCA with total loss of LHSI in state A which has been analysed in Sub-chapter 13.4.5.3. The consequences can also be bounded by SB-LOCA with total loss of LHSI in state A.

13.4.5.4.5 Conclusions

The results show that the automatic actions of reactor protection systems and operator actions can take the plant to its final state. The acceptance criteria are met.

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

In the accident of loss of RHR or failure of recovery of RHR after LOOP in state C or D, the decay heat cannot be removed by RHR system.

If the primary system is open, the coolant keeps evaporating due to decay heat and it may cause core level drop. SI signal can be triggered by "RCP [RCS] loop level low 1". Then safety injection can be used to compensate primary coolant inventory.

Decay heat is finally removed by EHR [CHRS], so as to reach the DEC-A final state. If the primary system is open, the consequences can be bounded by SB-LOCA with total loss of LHSI in shutdown state in Sub-chapter 13.4.5.4.

If the primary system is not open, the secondary side can be used to remove the decay heat. The consequences can be bounded by SBO in power operation which has been analysed in Sub-chapter 13.4.5.6.

13.4.5.6 SBO (State A to F)

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

If the primary system is not open, the bounding situation is SBO in state A.

If the primary system is open, the bounding situation is SBO in state D, in which the decay heat is the highest.

13.4.5.6.1 SBO (State A)

13.4.5.6.1.1 Description of the Accident

A SBO accident 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.

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

a) Main Feedwater System (ARE [MFFCS]);

b) Startup and Shutdown Feedwater System (AAD [SSFS]);

c) Emergency Feedwater System (ASG [EFWS]);

d) Chemical and Volume Control System (RCV [CVCS]);

e) Safety Injection System (RIS [SIS]);

f) Component Cooling Water System (RRI [CCWS]);

g) Essential Service Water System (SEC [ESWS]);

h) Reactor coolant pump;

i) Ventilation System;

j) Battery Charger;

k) Fuel Pool Cooling and Treatment System (PTR [FPCTS]);

l) Extra Cooling Water System (ECS).

SBO is an overheating DEC-A accident which will cause primary system overpressure. After an SBO accident happens, the three reactor coolant pumps stop working and coast down. Then, the “Low RCP pump speed” signal will trigger Reactor Trip (RT) for the core protection. With the reactor coolant pump trip and turbine trip, the

primary pressure increases and may reach the opening threshold of the PSVs. With the loss of ARE [MFFCS], AAD [SSFS] and ASG [EFWS], all SGs are no longer fed, the secondary side pressure increases and then the VDA [ASDS] open 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]. As a result, the water levels of the SGs constantly decrease. If no effective measures are taken, the SGs will dry up, and the pressure and temperature of primary system will increase rapidly. The coolant of primary system will steadily drain away because of the open PSVs, which may lead to fuel and clad damage. The UK HPR1000, SBO Diesel Generators (DGs) are designed and used to deal with an SBO accident. After 30 minutes following the RT signal, the SBO DGs are started by the operator for the supply of electricity to the ASG [EFWS], VDA [ASDS], ventilation systems, I&C systems and other protection systems or relative auxiliary systems. With these systems, the decay heat removal can be maintained. The pressure and temperature of the primary system can reach appropriate steady state values. In the long term, the design of reactor pump sealing is requested to keep tightness in this condition.

In addition, the cooling function of the ECS [ECS] is guaranteed to operate for 3 hours after the RT signal. One train of SBO diesel generator is switched from ASG [EFWS] to PTR [FPCTS] to remove the decay heat from spent fuel pool (SFP).

13.4.5.6.1.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.6.1.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (1.645σ uncertainties on the “B+C term”) is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of SBO accident.

1) The RT is triggered by the “Low RCP pump speed” signal;

2) The PZR safety valve sets are used to limit the RCP [RCS] pressure;

3) The VDA [ASDS] open automatically when the SG pressure reach “SG pressure high 1” to limit the secondary pressure.

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from the Main Control Room is assumed to be performed 30 minutes after the first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal.

1) Thirty minutes after the RT signal, start-up of two SBO Diesel Generators (SBO DGs), then start-up of the two ASG [EFWS] pumps in trains A and B;

2) One hour after the RT signal, opening of the ASG [EFWS] collecting pipe;

3) Two hours after the RT signal, the operator manually cools down the primary system {

}.

4) Three hours after the RT signal, the operator manually switches one train of SBO diesel generator from the ASG [EFWS] to the PTR [FPCTS] to remove the residual spent fuel heat.

After the above measures are taken, the following final state is achieved:

a) Ensure the sub-criticality of the core (through the automatic RT and limited cooldown operation, the addition of borated water is not necessary);

b) Use the ASG [EFWS] and VDA [ASDS] system to ensure decay heat removal;

c) Remain the radioactive release controllable (realised through the above measures);

d) Ensure the heat removal from SFP.

13.4.5.6.1.4 Results

The initial progression of the accident sequences is similar to the LOOP, which is characterised by a quick reactor trip, a natural circulation is established in the RCP [RCS], the VDA [ASDS] is used to remove heat from the secondary side at “SG pressure high 1” signal and no water refilling can be performed for the SGs at this time.

The actuation of the ASG [EFWS] pumps in trains A and B, results in the increase of the water level in the related SG to the nominal value, while the water level in the other SG keeps decreasing.

The ASG [EFWS] connecting pipes are opened 1 hour after RT signal, the water can be supplied to all SGs, and then the water level in the SG, which initially has no water supply, begins to increase quickly.

Two hours after the RT signal, the VDA [ASDS] system is used for cooling, with continuous cooling, the pressure and temperature of primary system can reach a proper and steady value. In the long term, the design of reactor pump sealing is

requested to keep tightness in this condition, and the final state is reached.

Three hours after the RT signal, one train of the SBO diesel generator is switched to support the PTR [FPCTS] (from ASG [EFWS]). One train of the PTR [FPCTS] can sufficiently cool the spent fuel pool, which can be enveloped by the accident sequence in Sub-chapter 13.4.5.7. In addition, the capacity of one train of the ASG [EFWS] is sufficient to supply water to all SGs.

13.4.5.6.1.5 Conclusions

As is shown in the analysis results, the core uncovery does not occur during the whole process of the accident, the pressure and temperature of the primary system are kept low enough to maintain the reactor pump seals, and the core decay heat can be removed sufficiently. The acceptance criteria are met for SBO accident (state A) [8].

13.4.5.6.2 SBO (State D)

13.4.5.6.2.1 Description of the Accident

The SBO (in shutdown condition) refers to the total loss of normal AC power distribution system and emergency AC power distribution system caused by LOOP with the failure of three EDGs in state D. The EDG failure may be caused by Common Cause Failure (CCF).

The state D refers to the Maintenance Cold Shutdown (MCS) condition with RCP [RCS] open. Due to the open status of the RCP [RCS], the SGs cannot be used for core decay heat removal. The condition to be considered in this section is the SBO accident occurring when the primary loop is fully open in state D.

In this operation mode:

a) The primary system is fully open;

b) The primary water level is equal to or higher than the minimum working water level for the operation of the RIS [SIS] in RHR mode;

c) The boron concentration of the reactor coolant is equal to or higher than the boron concentration required in refuelling mode;

d) The RIS [SIS] is in RHR mode and is connected with the RCP [RCS]. At this time, the heat in the RCP [RCS] is removed by the RIS [SIS] in RHR mode;

e) The average temperature in the primary loop is between 10°C and 60°C;

f) The primary pressure is 0.1 MPa abs.;

g) All RCP [RCS] pumps stop operation;

h) The SGs are not available.

When there is no other additional power supply, the following key systems will

become unavailable:

a) ARE [MFFCS];

b) AAD [SSFS];

c) RCV [CVCS];

d) RIS [SIS];

e) RRI [CCWS];

f) SEC [ESWS];

g) RCP [RCS] pump;

h) Ventilation system;

i) Battery charger;

j) PTR [FPCTS];

k) ECS [ECS].

13.4.5.6.2.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.6.2.3 Analysis Methods

The conservative assumptions are considered for main initial parameters, system parameters and time delay. LOOP, single failure and preventive maintenance assumption are not considered during accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (2σ uncertainties on the “B+C term”) is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of SBO accident.

1) In the long term of the accident, the water temperature of the IRWST does not exceed 120°C and the RHR of the core is ensured through the EHR [CHRS] and ECS [ECS] which are available latest at the time of 3 hours after the SBO accident and powered by the SBO diesel generator;

2) The RHR of the SFP is ensured by the PTR [FPCTS] and ECS [ECS] powered by the SBO diesel generator;

3) Since there are 2 SBO diesel generators available, one SBO diesel generator supplies the LHSI and the other SBO diesel generator supplies the EHR [CHRS], PTR [FPCTS] and ECS [ECS].

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from the Main Control Room is assumed to be performed 30 minutes after the first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal.

1) The operator starts the SBO emergency power supply manually 30 minutes after the SBO accident;

2) The LHSI pump in train A or train B is available 60 minutes after the SBO accident considering the starting time of supporting systems;

3) The PTR [FPCTS] is available 3 hours after the SBO accident considering the starting time of supporting systems and the time of PTR [FPCTS] reaching full flow, ensuring that the RHR of the SFP can be removed.

After the above measures are taken, the following final state is achieved:

a) Use the LHSI pump in train A or train B to ensure decay heat removal;

b) Remain the radioactive release controllable (realised through the above measures);

c) Ensure the heat removal from SFP.

13.4.5.6.2.4 Results

The SBO diesel generators have a small-scale power supply capacity. As their configurations are different from those of the EDGs, it is not necessary to consider the CCF with the EDGs.

The SBO diesel generators are manually connected and activated in the MCR. In the analysis, it is assumed that this measure is not taken within the first 30 minutes and the LHSI pump in train A or train B is not started within the first 60 minutes after the SBO accident.

It is conservatively assumed that the time required for the reactor to reach state D (primary loop fully open) is 48 hours after shutdown. To be conservative, only the latent heat of water vaporisation is taken into consideration. According to the analysis of the primary water inventory in state D, the water inventory that can be evaporated is from the minimum water level (3/4 of the mid-plane water level in the loop) to the top of active part of the core. The calculation shows that the existing water inventory is far more than the evaporation consumption within an hour after the accident, it can be ensured that the core will not be uncovered during the time from the SBO accident

occurring to the LHSI starting.

After the SBO diesel generators are activated, the following key measures will be taken (manually) to reach the final state. In this state, the reactor will be maintained until the offsite power is recovered:

a) Activate SBO emergency power in the MCR;

b) Manually start the LHSI pump in train A or train B;

c) Manually start the cooling pump in the PTR [FPCTS] to recover SFP cooling.

d) In the long term, in order to limit the containment pressure, temperature and the IRWST water temperature, the containment heat is removed through the EHR [CHRS] and the EHR [CHRS] removes heat to the Ultimate Heat Sink (UHS) through the ECS [ECS]. The containment pressure, temperature and the IRWST water temperature during a SBO accident in state D can be bounded by those in the SB-LOCA with a total loss of LHSI in state A.

As a result, when the SBO accident occurs in state D, the reactor can still be kept in a safe state:

a) The sub-critical state has been guaranteed as a priority before the accident;

b) A sufficient margin is kept for the RHR from the core;

c) As long as the core is not uncovered and the containment integrity is not destroyed, the radioactive release meets the limit for DBC-4.

13.4.5.6.2.5 Conclusions

The analysis results show that after the SBO accident happens in state D, it can be ensured that the core will not be uncovered during the time from the SBO accident occurring to the LHSI starting. In the long term, the containment heat can be removed through the EHR [CHRS] so that the containment pressure, temperature and the IRWST water temperature can be limited [9].

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

13.4.5.7.1 Description of the Accident

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 switchboard. 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’s 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 shown in Sub-chapter 13.4.3.2 are adopted as targets.

13.4.5.7.3 Analysis Methods

The increase of the average SFP temperature resulting from the loss of the cooling system is calculated considering the residual heat of the fuel assemblies, and the volume of SFP compartment. The main assumptions and analysis condition is list below:

a) The analysis uses best-estimate assumptions for DEC-A events.

b) The following assumptions are considered in the analysis:

- SFP and PTR [FPCTS] pipes are considered as adiabatic.
- The decay heat which is released from the spent fuel is total absorbed by the water in the SFP.
- The initial SFP water temperature is considered as 60°C. This value covers all the states.
- Before the accident, RRI [CCWS] inlet temperature is 45°C.
- After SBO, one PTR [FPCTS] cooling train cooled by ECS [ECS] can be loaded in three hours to cool the SFP.

13.4.5.7.4 Results

After the initial events, if the ECS is launched successfully three hours later, the PTR [FPCTS] train A or train B can be restarted and operating again, the maximum SFP water temperature is 90.5°C.

The long term SFP cool down is ensured by this PTR [FPCTS] train in operation during the whole transient. The corresponding stabilized temperature is 82.1°C. The fuel assemblies are covered with water during the transient.

13.4.5.7.5 Conclusions

The analysis result shows that all the fuel assemblies are covered with water during the transient. Thus the acceptance criteria for this event are met [10].

13.4.5.8 ATWS due to RPS failure (State A)

Analysis for ATWS due to RPS signal failure will be provided in PCSR V1.

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 of the Accident

In an ATWS accident with loss of main feedwater, the reduction of feedwater flow rate leads to the inventory of the SGs decrease which triggers “SG level (narrow range) low 1” signal, which will result in reactor trip 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.

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

After turbine trips, the steam is discharged either by GCT [TBS] or VDA [ASDS]. The SGs water level decreases sharply and when the SGs tubes are uncovered, the heat transfer from the primary side to the secondary side decreases. This leads to a significant increase in the primary pressure and temperature which results in the opening of PSVs. After the RCP [RCS] pumps stop, the primary coolant flow rate decreases sharply and the primary temperature rises further. The core power decreases due to the negative feedback effect of the reactor coolant, thus slowing down the increasing rate of primary pressure and temperature.

The “SG level (wide range) low 2” signal initiates the ASG [EFWS]. The SG recovers and the heat exchange between the primary side and the secondary side increases, the primary temperature, pressure and pressuriser water level also begin to drop. The RBS [EBS] boron injection ensures that the core remains subcritical in the long term.

13.4.5.9.1.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. If the minimum Departure from Nucleate Boiling Ratio (DNBR) remains above the design limit, the criteria shown in Sub-chapter 13.4.3.2 are met. The primary highest pressure should be under 22MPa abs. to ensure the primary side remains intact.

13.4.5.9.1.3 Analysis Methods

COCO is used for nuclear data calculation. GINKGO is used to analyse the transient process. LINDEN is used for detailed DNBR analysis.

a) Initial Assumptions

1) The typical initial power is 102%FP.

2) The initial average temperature of the reactor coolant is set at a conservative

value.

3) The initial pressuriser pressure is set at a conservative value.

b) Functions Assumptions

1) The normal feedwater is totally lost at 0s.

2) All emergency feedwater pumps are available.

3) The pressuriser safety valve (PSV) opening pressure is set a conservative value.

c) Control and protection systems

1) The “rod position signal (at least 2 control rods cannot be inserted)” combined with RT signal triggers the ATWS signal.

2) The insertion effects of power compensation rods and temperature adjustment rods are not considered.

3) The “SG level (wide range) low 2” signal initiates the ASG [EFWS].

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

5) The ATWS signal initiates the RBS [EBS] automatically.

13.4.5.9.1.4 Results

This accident leads to a significant increase in the primary pressure and temperature.

It is mitigated through the negative feedback effect of the reactor coolant and PSV, GCT [TBS] or VDA [ASDS], ASG [EFWS] and RBS [EBS]. The negative feedback effect of the reactor coolant limit the core power, the PSV limit the primary pressure increasing, the GCT [TBS] or VDA [ASDS], ASG [EFWS] bring heat from the secondary side.

RCP [RCS] pumps stop, the primary coolant flow rate decreases sharply and the primary temperature rises further. Due to the negative feedback effect of the reactor coolant the core power decreases.

RBS [EBS] injection ensures the core remains subcritical in the long term.

The detailed analysis of this fault shows that the minimum DNBR is greater than the design limit. Therefore the fuel integrity will not be challenged following a loss of main feedwater ATWS. The calculated peak primary pressure does not exceed the maximum allowable pressure of 22.0 MPa abs. Therefore, this fault does not challenge the integrity of the RCP [RCS].

13.4.5.9.1.5 Conclusions

It is concluded that the acceptance criteria are met in ATWS-Loss of Main Feedwater

[11].

13.4.5.9.2 ATWS-Loss of Offsite Power

13.4.5.9.2.1 Description of the Accident

Loss of offsite power (LOOP) leads to loss of power for all auxiliary plant equipment, such as the RCP [RCS] pumps, condensate and main feedwater pumps, etc.

After LOOP, RCP [RCS] pumps coast down and coolant flow rate decreases. The RT signal is emitted on “low RCP [RCS] pumps speed” signal. However, although the RT signal has been transmitted, 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 may lead to a decrease in the DNBR margin. Finally, the core is cooled through natural circulation. The high rod position combined with RT signal lead to the triggering of the ATWS signal which initiates the RBS [EBS] operation.

The opening of the PSV limits the primary pressure rise, and the VDA [ASDS] ensures the removal of the secondary heat. When the SG water level decreases to the “SG level (wide range) low 2” signal, the ASG [EFWS] starts up to supply water to the SG. Boron injection by the RBS [EBS] ensures that the core is in the subcritical state in the long term. The ASG [EFWS] and RBS [EBS] are initiated according to the EDG reloading sequence following LOOP.

13.4.5.9.2.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target. If the minimum DNBR remains above the design limit, the criteria shown in Sub-chapter 13.4.3.2 are met.

13.4.5.9.2.3 Analysis Methods

COCO is used for nuclear data calculation. GINKGO is used to analyse the transient process. LINDEN is used for detailed DNBR analysis.

a) Initial Assumptions

1) The typical initial power is 102%FP.

2) The initial average temperature of the reactor coolant is set at a conservative value.

3) The initial pressuriser pressure is set at a conservative value.

b) Functions Assumptions

Non-emergency AC power is lost at 0 s, triggering:

1) RCP pumps trip until each loop builds natural circulation;

2) Unavailability of all main feedwater pumps;

3) Turbine trip.

The following plant control systems are all unavailable due to Loss of Offsite Power:

1) Steam discharge control;

2) Pressuriser electric heater.

The pressure set point of the PSV is the rated value.

c) Control and protection systems

1) The RCP pump rotating speed low 2 triggers the trip signal;

2) The rod position signal (at least 2 control rods cannot be inserted) triggers the ATWS signal;

3) The insertion effects of power compensation rods and temperature adjustment rods are not considered.

4) The ATWS signal initiates the RBS [EBS] automatically.

13.4.5.9.2.4 Results

After LOOP, RCP [RCS] pumps coast down and coolant flow rate decreases. The coolant flow rate decreases that lead to the heat transfer reducing between primary and secondary. The primary temperature and pressures rise rapidly. The opening of the PSV limits the primary pressure rise, and the VDA [ASDS] ensures the removal of the secondary heat. The ASG [EFWS] and RBS [EBS] are initiated according to the EDG reloading sequence following LOOP.

The detailed analysis of this fault shows that the minimum DNBR is greater than the design limit. Therefore the fuel integrity will not be challenged following ATWS-Loss of Offsite Power.

13.4.5.9.2.5 Conclusions

The minimum DNBR is greater than the design limit. It is concluded that acceptance criteria are met in ATWS- LOOP [12].

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

13.4.5.10.1 Description of the Accident

A small break located at the cold leg will lead to a decrease in coolant inventory which cannot be compensated by the RCV [CVCS]. The MHSI is assumed to be unavailable. The loss of primary coolant leads to a decrease in the RCP [RCS] pressure and the water level in the pressuriser. The “Pressuriser pressure low 2” signal triggers the reactor trip. After that, the turbine trip is triggered and the full load

isolation valves of the ARE [MFFCS] are closed automatically. The SGs are refilled with water by the ARE [MFFCS] system through the low load pipelines. 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. The RCP [RCS] pumps will stop due to the combination of the SI signal and "RCP [RCS] pump ΔP low 1" signal. The secondary pressure increases and is limited by the GCT [TBS]. When the GCT [TBS] is unavailable, the VDA [ASDS] is used to prevent overpressure of the secondary circuit. The "Pressuriser pressure low 3" signal triggers the SI signal. The SI signal activates the LHSI pump automatically and triggers the MCD 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 RIS accumulator or LHSI to perform injection. Therefore, mitigation of the accident relies on operator actions. 3 trains of the VDA [ASDS] are manually activated. Two RBS [EBS] pumps are manually activated to inject borated water into the RCP [RCS] for primary system depressurisation. In the course of primary system depressurisation, the RIS accumulator is manually isolated. In this analysis, the final state is defined as reaching the RIS [SIS] connection condition in RHR mode.

13.4.5.10.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.10.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (2σ uncertainties on the "B+C term") is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of the accident.

1) The RT is triggered by the "Pressuriser pressure low 2" signal;

2) The SI signal is triggered by the "Pressuriser pressure low 3" signal;

3) The MCD is triggered by the SI signal;

4) The RCP [RCS] pumps stops due to the combination of a SI signal and "RCP [RCS] pump ΔP low 1" signal;

5) 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.

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from the Main Control Room is assumed to be performed 30 minutes after the first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal.

1) Thirty minutes after the RT signal , the operator will manually actuate two trains of RBS [EBS];
2) Thirty minutes after the RT signal , the operator will manually open the VDA to cool down the primary system.

After the above measures are taken, the following final state is achieved:

a) Ensure the sub-criticality of the core (through the automatic RT and limited cooldown operation);
b) Use the ASG [EFWS] and VDA [ASDS] system to ensure decay heat removal;
c) Remain the radioactive release controllable (realised through the above measures).

13.4.5.10.4 Results

The primary pressure and coolant inventory decreases quickly after the break occurs. “Pressuriser pressure low 2” signal triggers the RT. The RT signal triggers the turbine trip and closes full load isolation valves of the ARE [MFFCS] automatically. After the RT, the primary pressure decreases. The “Pressuriser pressure low 3” signal triggers the SI signal which then triggers the MCD signal.

The operator starts 2 trains of RBS [EBS] pumps 30 minutes after the RT signal and opens 3 trains of VDA [ASDS] to cool down the primary system at the same time. After the LCD starts, the primary pressure decreases to the RIS accumulator injection pressure quickly and the RIS accumulator starts injection to increase the water level in the RPV. After that, the LHSI injection pressure is reached. The LHSI starts to inject borated water into the RCP [RCS], the primary temperature and pressure decrease continuously. When the RIS [SIS] connection condition in RHR mode is met, it is concluded that the final state is reached.

13.4.5.10.5 Conclusions

The results show that the automatic actions of reactor protection systems and operator actions can take the plant to its final state. The acceptance criteria are met [13].

13.4.5.11 Reactor Coolant Sealing Leakage Caused by TLOCC (State A)

13.4.5.11.1 Description of the Accident

The TLOCC accident in state A refers to the total loss of RRI [CCWS] and SEC [ESWS]. As a result, 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 failure of the reactor coolant pump sealing resulting in a break of the primary system, the maximum break flow is taken into account for this accident analysis;

f) 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 accident, the TLOCC results in the loss of sealing injection and loss of the thermal barriers, consequently leading to the trip of the reactor coolant pumps. The "Low RCP pump speed" signal triggers the RT. The RT signal leads to turbine trip (TT) 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", which starts the MHSI and LHSI system and initiates the MCD operation automatically, {
}. 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 Safety Chilled Water System (DEL [SCWS]), and then the LHSI pumps of trains A and B are available.

After the MCD operation, the RCP [RCS] pressure is still too high to allow injection by RIS accumulators or LHSI (All MHSI are unavailable). Therefore, it is necessary to perform the operator actions including actuation of the RBS [EBS] and LCD for the mitigation of the TLOCC accident. In order to decrease the primary pressure to the injection pressure of the RIS accumulators and LHSI, the operator actuates two trains of the RBS [EBS] for RCP [RCS] boration 30 minutes after the RT signal, and then performs the LCD 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] and

ECS [ECS] are started manually to cool the water of the IRWST and containment as the ultimate heat sink. The IRWST water temperature remains within the limit and the containment integrity is ensured.

13.4.5.11.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.11.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (2σ uncertainties on the “B+C term”) is used.

c) Functions Assumptions

The following automatically or manually activated functions/systems are used for the mitigation of TLOCC accident.

1) Reactor coolant pump

The reactor coolant pumps are stopped due to the loss of thermal barriers and pump sealing injection.

2) Reactor trip

The RT signal is actuated on “Low RCP pump speed”.

3) Turbine trip

The turbine trip is triggered by the RT signal.

4) SI

The SI signal is triggered by “Pressuriser pressure low 3”.

5) MCD

The MCD is triggered by the SI signal.

6) 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.

d) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from Main Control Room is assumed to be performed 30 minutes after the first significant signal, the first local operator action is assumed to be performed 60 minutes after the first significant signal.

1) RBS [EBS]

The RBS [EBS] is started up manually 30 minutes after the RT signal to ensure the reactor is in the sub-critical state during the cooling stage.

2) LCD

Thirty minutes after the RT signal, the operator performs the LCD through the VDA [ASDS].

13.4.5.11.4 Results

Due to TLOCC, reactor coolant pumps stop working and begin to coast down, and the RCP [RCS] water inventory starts to decrease due to the sealing leakage. The RT signal is actuated on “low RCP pump speed” signal, leading to rod drop, turbine trip and isolation of the ARE [MFFCS] full load lines. With the coolant inventory and primary pressure decreasing, the “Pressuriser pressure low 3” triggers the SI signal which actuates the MCD{ }.

The operator starts up 2 trains of RBS [EBS] 30 minutes after the RT signal, and then opens 3 trains of VDA [ASDS] to depressurize the primary side. When the primary pressure is lower than the injection pressure of the RIS accumulators, the RIS accumulator begins to inject. When the primary pressure is lower than the injection pressure of the LHSI, the LHSI in train A and B begin to inject water into the core. In the long term, the EHR [CHRS] and ECS [ECS] are started manually to cool the IRWST and containment as the ultimate heat sink. The IRWST temperature remains within the limit and the containment integrity is ensured.

13.4.5.11.5 Conclusions

As it is shown in the analysis results, the core uncovery does not occur during the whole process of the accident, the core decay heat is removed continuously. The acceptance criteria are met in TLOCC with a reactor coolant pump sealing leakage accident (state A) [14].

13.4.5.12 TLOCC (State D)

13.4.5.12.1 Description of the Accident

Total Loss of Cooling Chain (TLOCC) refers to the total loss of Component Cooling Water System (RRI [CCWS]) and Essential Service Water System (SEC [ESWS]). As the main consequences, the following systems will be lost:

a) Chemical and Volume Control System (RCV [CVCS]);

b) All Medium Head Safety Injection (MHSI) series;

c) Train C of the Low Head Safety Injection (LHSI);

d) All Residual Heat Removal (RHR) exchangers.

It's assumed that the TLOCC occurs in Maintenance Cold Shutdown (MCS) condition (state D).

13.4.5.12.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are used as target.

13.4.5.12.3 Analysis Methods

Conservative assumptions are considered for main initial parameters, system parameters and time delay. LOOP, single failure and preventive maintenance assumption are not considered during accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative heat curve (2σ uncertainties on the "B+C term") is used for the core decay heat.

c) Functions Assumptions

The LHSI is actuated by the "RCP loop level low 1" signal during the mitigation of TLOCC accident.

After the above measures are taken, the following final state is achieved:

a) Use the LHSI system to ensure decay heat removal;

b) Remain the radioactive release controllable (realised through the above measures);

c) Ensure the heat removal from SFP.

13.4.5.12.4 Results

After the TLOCC accident occurs, the average coolant temperature increases due to the loss of the RIS [SIS] in RHR mode. When the saturation temperature is reached, heat is removed through coolant evaporation. Due to the decrease of the water level in the RCP [RCS] loop, the LHSI will be actuated by the "RCP loop level low 1" signal. It has sufficient capacity to compensate for the evaporation of coolant. As a result, the RCP [RCS] is not uncovered during a TLOCC (state D).

Due to loss of the cooling chain, the RIS [SIS] in RHR mode is not recovered. The

EHR [CHRS] in spraying mode is actuated to control the containment pressure. The EHR [CHRS] removes heat to the UHS through the ECS [ECS].

13.4.5.12.5 Conclusions

The water inventory in the RIS [SIS] and IRWST can ensure the core remains fully submerged during the TLOCC accident. The integrity of the containment can be guaranteed by the EHR [CHRS] and ECS [ECS] [15].

For SFP, heat removal is ensured by the PTR [FPCTS] and ECS [ECS].

It is concluded that the acceptance criteria are met in TLOCC in state D.

13.4.5.13 Loss of three PTR [FPCTS] trains (State A to F);

13.4.5.13.1 Description of the accident

The loss of three trains of the PTR [FPCTS] in the SFP leads to a temperature increase of SFP water and the fuel building atmosphere. As the main consequence, the SFP is boiling, and the fuel building is becoming over-pressured. In case of this accident, the operator performs the water makeup through the ASP [SPHRS] tank or the external water source. Then, the depressurization of the fuel building can be realized by the manual opening of damper or the passive opening of the rupture disc.

13.4.5.13.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets.

13.4.5.13.3 Analysis Methods

a) Initial Assumptions

The initial temperature of SFP water is 50 °C, the initial water level of SFP is 16.9 m.

b) Decay Heat Assumption

The accident is assumed to happen in reactor abnormal completely discharged state, which results in the maximum decay heat for the accident analysis.

c) Functions Assumptions

1) SFP water makeup

Thirty minutes after the accident, when the SFP level begins to decrease, the operator opens the valves for the SFP water makeup via the ASP [SPHRS] tank.

2) Fuel building depressurization

Thirty minutes after the accident, the operator opens the damper to depressurize the fuel building; when the pressure difference between the fuel building and atmosphere is greater than { }, the rupture disc is opened passively.

13.4.5.13.4 Results

When SFP loses three trains of PTR cooling, the temperature of SFP water increases and finally arrives at the boiling temperature several hours later. The decay heat of SFP is removed through water makeup and evaporation mode. Considering the decay heat in reactor abnormal completely discharged state, the maximum water evaporation rate can be calculated. The manual operations are assumed to be performed thirty minutes after the accident. When the SFP level decreases, the operator can open the water makeup valve locally to perform the gravity water makeup from ASP [FPCTS] tank to the SFP. And the makeup is stopped if the SFP level increases above the normal level to avoid the irreversible water loss through the overflow lines. The flow rate of water makeup from ASP [FPCTS] is greater than the SFP water evaporation rate. So the fuel assemblies are covered during the whole accident course. As the fuel building pressure increases, thirty minutes after the accident, the operator opens the damper locally to depressurize the fuel building. Even if the damper is failed to open, the passive rupture disc can open to avoid the over-pressure of the fuel building.

13.4.5.13.5 Conclusions

With the water makeup from the ASP tank or the external water source, the safety water level of SFP is ensured and the fuel assemblies of SFP are covered during the whole process. The sub-criticality of the fuel assemblies is ensured by the design of spent fuel storage rack and “covering of spent fuel assemblies”. The removal of decay heat from SFP is ensured via makeup and evaporation of the SFP water in the long term.

13.4.5.14 LUHS for 100 hours (state A and B);

LUHS during 100 hours (state A and B) refers to the total loss of the RRI/SEC [CCWS/ESWS] or the total loss of the ultimate heat sink in states A and B without leakage from the RCP [RCS] pump sealing, and it belongs to the DEC-A sequences. The related DEC-A feature is the refilling of the ASG [EFWS] tanks.

In the case that LUHS occurs in state A, the removal of decay heat after RT depends on the automatic opening of the VDA [ASDS] and the feedwater to the SG which is assured by the ASG [EFWS]. In order to ensure the capacity of the ASG [EFWS] tanks to be sufficient for the removal of decay heat over 100 hours, it is necessary to refill the ASG [EFWS] tanks.

Based on qualitative judgement, the 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 tank. The capacity of the ASP tank is designed for decay heat removal for 76 hours in LUHS conditions in state A.

It is concluded that the DEC-A final state can be achieved by the mitigation actions mentioned above in a LUHS accident for 100 hours in state A.

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 needing 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 tanks. Thus, the case in state B can be enveloped by that of state A. The detailed analysis will be performed in PCSR v1.

13.4.5.15 Uncontrolled Primary Water Level Drop without SI Signal from RPS (state D)

13.4.5.15.1 Description of the Accident

In the normal cold shutdown condition of plant, the core decay heat is removed continuously by the RIS [SIS] in Residual Heat Removal (RHR) mode. The uncontrolled primary water level drop accident is assumed to happen in state D. State D is described as follows:

a) The RCP [RCS]) is not closed and not able to be pressurized;

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

c) The heat in the RCP [RCS] is removed by the RIS system in RHR mode;

d) The RCP [RCS] coolant average temperature is between 10 °C and 60 °C;

e) The RCP [RCS] pressure is atmospheric pressure.

In state D, the RCP [RCS] level decreases continuously when a failure of the water level control occurs. It may lead to the cavitation of the RIS/RHR pumps. With the RCP [RCS] level decreasing, the “RCP [RCS] loop level low 1” threshold is reached, however the Safety Injection (SI) signal is not sent because of the failure of the RPS. Without any other protection measures, the RIS/RHR pumps will be damaged and the core will eventually be uncovered.

In order to deal with this accident, a diversified “RCP [RCS] loop level low 1” signal is emitted from the Diversity Actuation System (KDS [DAS]) to actuate the RIS system. With the actuation of MHSI, the RCP [RCS] water level begins to increase, and the core decay heat can be removed by the RIS/RHR in the long term.

13.4.5.15.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets. Besides, the RIS/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 the RIS/RHR during the whole accident course.

13.4.5.15.3 Analysis Method

Quantitative assessment is used to analyse the process of this accident.

a) Initial Assumption

The accident is assumed to happen in the MCS state, and the RCP [RCS] water level is assumed to be the lowest level of the operation interval of RIS/RHR. The primary coolant average temperature is 60 °C. During the accident analysis, the maximum letdown flow rate of Chemical and Volume Control System (RCV [CVCS]) is considered.

b) Decay Heat Assumption

The decay heat curve (2σ uncertainties on "B+C term") is used during the analysis.

c) Function Assumption

1) RIS

The RIS is actuated depending on the diversified "RCP [RCS] loop level low 1" signal.

2) RCV letdown isolation

After the diversified SI signal, the RCV [CVCS] letdown line is isolated.

13.4.5.15.4 Results

The water inventory between the diversified "RCP [RCS] loop level low 1" threshold and the RIS/RHR pump cavitation level can be calculated. The 75t/h is considered as the RCV [CVCS] letdown flow rate. By calculation, the time between reaching the "RCP [RCS] loop level low 1" threshold and RIS/RHR pump cavitation level is greater than the delay time of MHSI actuation. After the actuation of MHSI, the water makeup flow rate of MHSI is greater than the RCV [CVCS] letdown flow rate.

Consequently, the RCP [RCS] water level drop stops before reaching the RIS/RHR pump cavitation level, and the RCP [RCS] water level begins to increase after the actuation of MHSI. Besides, the RCV [CVCS] letdown line is isolated after the diversified SI signal. The core decay heat is removed through RIS/RHR in the long term.

13.4.5.15.5 Conclusions

The analysis shows that diversified protection signals from KDS [DAS] can mitigate this accident. It is concluded that the acceptance criteria are met [16].

13.4.5.16 Multiple SG Tubes Rupture (10 tubes) (State A)

13.4.5.16.1 Description of the Accident

Multiple steam generator tubes ruptures (SGTRs) leads to a decrease of primary pressure and a loss of primary coolant. The coolant is transferred from the primary system to the Affected Steam Generator (SGa), which contaminates the secondary side and induces a fast increase of the SGa level. As a main consequence, the activity of the primary system is transferred to the SGa due to the multiple rupture and possibly discharged to the environment through the VDA [ASDS].

In the case of multiple SGTRs, some automatic protection functions are activated to mitigate the accident, such as RT, turbine trip, isolation of ARE [MFFCS]. Operator actions are performed 30 minutes after the first significant signal to reach the DEC-A final state. The operator confirms the isolation of SGa and performs the manual cooldown of the RCP [RCS] via the VDA [ASDS] and ASG [EFWS] of integral SG loops. If the RCP [RCS] pressure doesn't reach the RHR connecting condition, the VDA [ASDS] of SGa is used to depressurize the RCP [RCS]. Before the opening of the VDA [ASDS], the Steam Generator Blowdown System (APG [SGBS]) transfer line is used to limit the water level and thus avoid overflow in the SGa. With these automatic and manual protection functions, the activity release to the environment can be limited finally.

13.4.5.16.2 Acceptance Criteria

The acceptance criteria shown in Sub-chapter 13.4.3.2 are adopted as targets.

13.4.5.16.3 Analysis Methods

The LOCUST code is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative heat curve (1.645σ uncertainties on the "B+C term") is used.

c) Functions Assumption

The automatic and manual safety functions used to deal with this accident are introduced as follows.

1) RT

The RT occurs on "pressuriser pressure low 2" signal.

2) Turbine Trip

The turbine trip is initiated after RT.

3) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT, the low load line of ARE [MFFCS] is isolated on “SG level (narrow range) high 0 and RT” signal.

4) SI

The SI is actuated on “pressuriser pressure low 3” signal.

5) MCD

The MCD is performed automatically after the SI signal.

6) RCP [RCS] pumps

The RCP [RCS] pumps trip on “RCP [RCS] pump ΔP low 1 and SI” signal.

7) RCV [CVCS]

After MCD, the RCV [CVCS] charging lines and RCP [RCS] pumps sealing water injection are isolated on “SG level (narrow range) high 2” signal. The RCV [CVCS] letdown is isolated on “pressuriser level low 1 and RT” signal.

8) Main Steam Isolation Valve (MSIV)

The MSIV are closed on “SG level (narrow range) high 2” signal after MCD.

9) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1”. The setpoint of VDA [ASDS] in SGa is increased to { } between the MHSI delivery pressure and MSSV [MSSV] opening setpoint on “SG level (narrow range) high 2” signal after MCD.

10) ASG [EFWS]

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

11) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from MCR is assumed to be performed 30 minutes after the first significant signal.

The operator confirms the total isolation of SGa, closes the MHSI in unaffected loops, and actuates two RBS [EBS], then performs the manual RCP [RCS] cooldown { }. When the core outlet temperature is lower than { }, the MHSI in the affected loop is closed. When the RCP [RCS] pressure decreases below { }, the RIS accumulators are isolated. And the APG [SGBS] transfer line is used to reduce the water inventory of SGa. Then, the operator depressurizes the RCP [RCS] via the VDA

[ASDS] of SGa.

13.4.5.16.4 Results

In the case of multiple SGTRs, a fast primary pressure decrease occurs, RT is initiated on “pressuriser pressure low 2” signal, the full load lines of ARE [MFFCS] are isolated and the turbine trip is initiated automatically after the RT. The level of SGa increases due to the leakage from primary side to SGa continuously. The ARE [MFFCS] low load line of SGa is isolated on “SG level (narrow range) high 0” signal.

Due to the loss of primary coolant, the pressuriser level decreases and the RCV [CVCS] letdown lines are isolated on the “pressuriser level low 1” signal. The SI is actuated on “pressuriser pressure low 3” signal, and an automatic MCD { }.

At the end of MCD, because of the “SG level (narrow range) high 2” signal, the MSIV is closed and the VDA [ASDS] setpoint of the SGa is increased to { } (between the MHSI delivery pressure and MSSV [MSSV] opening setpoint). This signal also actuates the isolation of the RCV [CVCS] charging lines and RCP [RCS] pumps sealing water injection.

The operator performs manual actions at about 1800.0 seconds after the first significant signal, confirms the total isolation of SGa, closes the MHSI in unaffected loops, and actuates two RBS [EBS], then performs the manual RCP [RCS] cooldown { }. When the core outlet temperature decreases below { }, the operator closes the MHSI in the affected loop.

When the RCP [RCS] pressure decreases below { }, the RIS accumulators are isolated. Then, the operator opens the APG [SGBS] transfer line to reduce the water inventory of SGa. The VDA [ASDS] of SGa is used to depressurize the RCP [RCS], so as to reach the RHR connecting condition. Finally, the RHR is connected to continuously remove the decay heat in the long term.

13.4.5.16.5 Conclusions

As results described above, with automatic and manual functions applied in the multiple SG tubes rupture (10 tubes) accident, overflow does not occur in the SGa. The source term and radiological consequences are assessed in Sub-chapter 13.4.6 and Sub-chapter 13.4.7. It is concluded the acceptance criteria are met [17].

13.4.5.17 MSLB with SGTR (1 tube) in the Affected SG (State A)

13.4.5.17.1 Description of the Accident

Main Steam Line Break (MSLB) with SGTR (one tube) leads to a fast depressurization of the secondary side and a loss of the primary coolant, which is an overcooling accident for the core. The MSLB is assumed to be located at the

downstream of the MSIV. It is also assumed the MSLB leads to one SGTR in the same loop. As a main consequence, the activity of primary system is transferred to the SGa due to the SGTR and discharged to the environment through the MSLB and VDA [ASDS].

In the case of MSLB with SGTR, some automatic protection functions are actuated to measure the accident, such as RT, turbine trip, isolation of ARE [MFFCS]. Besides, operator actions are performed 30 minutes after the first significant signal to reach the final state of DEC-A. The operator confirms the isolation of SGa and performs the manual cooldown of RCP [RCS] via VDA [ASDS] and ASG [EFWS] of integral SG loops. If the RCP [RCS] pressure doesn't reach the RHR connecting condition, the VDA [ASDS] of SGa is used to depressurize the RCP [RCS]. Before the opening of the VDA [ASDS], the APG [SGBS] transfer line is used to limit the water level and thus avoid overflow in the SGa. With these automatic and manual protection functions, the activity release to the environment is stopped.

13.4.5.17.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are adopted as targets.

13.4.5.17.3 Analysis Methods

LOCUST is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (1.645σ uncertainties on the "B+C term") is used.

c) Functions Assumption

The automatic and manual safety functions used to mitigate this accident are introduced as follows.

1) RT

The RT occurs on "pressure drop of SG high 1" signal.

2) Turbine Trip

The turbine trip is initiated after RT.

3) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT, the low load line of ARE [MFFCS] is isolated on "pressure drop of SG high 2" signal.

4) SI

The SI is actuated on “pressuriser pressure low 3” signal.

5) RCP [RCS] pumps

The RCP [RCS] pumps stop on “RCP [RCS] pump ΔP low 1 and SI” signal.

6) RCV [CVCS]

The RCV [CVCS] letdown is isolated on “pressuriser level low 1 and RT” signal.

7) MSIV

The MSIV are closed on “pressure drop of SG high 1” signal.

8) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1”.

9) ASG [EFWS]

The ASG [EFWS] is actuated on “SG level (wide range) low 2” signal.

10) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from MCR is assumed to be performed 30 minutes after the first significant signal.

The operator confirms the total isolation of SGa, actuates two RBS [EBS], then performs the manual RCP [RCS] cooldown { }. When the core outlet temperature is lower than { }, the MHSI in the affected loop is closed. When the RCP [RCS] pressure decreases below { }, the RIS accumulators are isolated. And the APG [SGBS] transfer line is used to reduce the water inventory of SGa. Then, the operator depressurizes the RCP [RCS] via the VDA [ASDS] of SGa.

13.4.5.17.4 Results

In the case of MSLB with SGTR, a fast secondary pressure decrease occurs. RT is initiated on “pressure drop of SG high 1” signal, and this signal also actuates the closing of MSIV. The full load lines of ARE [MFFCS] are isolated and the turbine trip is initiated automatically after the RT. The low load line of ARE [MFFCS] is isolated on “pressure drop of SG high 2” signal. The ASG [EFWS] are actuated on “SG level (wide range) low 2” signal. Because of the loss of primary coolant, the RCV [CVCS] letdown is isolated on “pressuriser level low 1 and RT” signal. After the closing of the MSIV, the secondary pressure increases to the VDA [ASDS] setpoint and the VDA [ASDS] opens automatically.

At about 1800.0 seconds after the first significant signal, the operator performs the

isolation of the SGa, including the ARE [MFFCS] and ASG [EFWS] isolation, VDA [ASDS] setpoint increase and so on. In order to balance the pressure difference between RCP [RCS] and SGa, the operator isolates the RCV [CVCS] charging lines and RCP [RCS] pumps sealing water injection. Then the operator actuates two RBS [EBS] and performs RCP [RCS] cooldown {

}. During the cooldown process, the SI signal emitted on “pressuriser pressure low 3” signal.

When the RCP [RCS] pressure is decreased below { }, the RIS accumulators are isolated. The APG [SGBS] transfer line is used to limit the water level and avoid the overflow of SGa. Then, the VDA [ASDS] of SGa is used to decrease the RCP [RCS] pressure to reach the RHR connecting value. With the connection of RHR, the core decay heat can be removed in the long term.

13.4.5.17.5 Conclusions

With automatic and manual protecting functions applied in MSLB with SGTR accident, overflow does not occur in the SGa. The source term and radiological consequences are assessed in Sub-chapter 13.4.6 and Sub-chapter 13.4.7. It is concluded the acceptance criteria are met [18].

13.4.5.18 SGTR (1 tube) with VDA [ASDS] Stuck Open in the SG Affected (State A)

13.4.5.18.1 Description of the Accident

A steam generator tube Rupture (SGTR) leads to the loss of primary coolant, which is transferred from primary side to SGa. The secondary side is contaminated and its pressure increases to the VDA [ASDS] setpoint which leads to the automatic opening of the VDA [ASDS]. The VDA [ASDS] in SGa loop is assumed to remain stuck open since it opened, which consists a non-isolable flow path between primary system and the environment. A main consequence is that, the activity 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 stop the continuous activity release to the environment, the operator actuates two RBS [EBS] and performs the manual LCD via the VDA [ASDS] and ASG [EFWS] of unaffected SG. When the RHR connecting conditions are reached, the RHR is connected to the primary system. Finally, the activity release to the environment is stopped.

13.4.5.18.2 Acceptance Criteria

The acceptance criteria mentioned in Sub-chapter 13.4.3.2 are adopted as targets.

13.4.5.18.3 Analysis Methods

LOCUST is used for the accident analysis.

a) Initial Assumptions

The key initial parameters are penalized by considering their uncertainties.

b) Decay Heat Assumption

A conservative decay heat curve (1.645σ uncertainties on the “B+C term”) is used.

c) Functions Assumption

The automatic and manual functions used to mitigate this accident are introduced as follows.

1) RT

The RT occurs on “SG level (narrow range) high 1” or “pressuriser pressure low 2” signal.

2) Turbine Trip

The turbine trip is initiated after RT.

3) ARE [MFFCS]

The full load lines of ARE [MFFCS] are isolated after RT, the low load line of ARE [MFFCS] is isolated on “pressure drop of SG high 2” signal.

4) SI

The SI is actuated on “pressuriser pressure low 3” signal.

5) MCD

The MCD is performed automatically after the SI signal.

6) RCP [RCS] pumps

The RCP [RCS] pumps stop on “RCP [RCS] pump ΔP low 1 and SI” signal.

7) RCV [CVCS]

The RCV [CVCS] charging lines are isolated on “SG pressure low 4 and SI” signal. The RCV [CVCS] letdown is isolated on “pressuriser level low 1 and RT” signal.

8) MSIV

The MSIV is closed on “pressure drop of SG high 1” signal.

9) VDA [ASDS]

The VDA [ASDS] opens automatically when the SG pressure reaches “SG pressure high 1”.

10) ASG [EFWS]

The ASG [EFWS] is actuated on “SG level (wide range) low 2” signal.

11) Operator Actions

Some operator actions are performed to reach the final state of DEC-A. The first operator action from MCR is assumed to be performed 30 minutes after the first significant signal.

The operator confirms the total isolation of SGa, actuates two RBS [EBS], and performs the manual LCD via VDA [ASDS] and ASG [EFWS] in unaffected SG. When the RCP [RCS] pressure decreases below { }, the RIS accumulators are isolated. Finally, the RHR is connected to the primary system to continuously remove the decay heat.

13.4.5.18.4 Results

When the SGTR happens, it is detected on the “high activity” signal from secondary side. An automatic RT occurs on "pressuriser pressure low 2" signal. The full load lines of ARE [MFFCS] are isolated and the turbine trip is initiated automatically after the RT.

As the primary coolant loses continuously, the RCV [CVCS] letdown is isolated on “pressuriser level low 1 and RT” signal. Since the VDA [ASDS] opens automatically, the VDA [ASDS] in SGa loop is assumed to be stuck open, which leads to a fast decrease of secondary side pressure. The MSIV closes on “pressure drop of SG high 1” signal, and the low load line of ARE [MFFCS] is isolated on “pressure drop of SG high 2” signal. Later on, the automatic SI occurs on “pressuriser pressure low 3” signal, and an automatic MCD is initiated after the SI signal. The RCV [CVCS] charging line is isolated on” SG pressure low 4 and SI” signal.

At about 1800.0 seconds after the first significant signal, the operator actuates two RBS [EBS] and performs the manual LCD via the VDA [ASDS] and ASG [EFWS] of unaffected SG. The primary coolant temperature decreases rapidly lower than { }. After confirmation of low core outlet temperature, enough saturation margin and pressuriser level high enough, the operator closes MHSI. When the RCP [RCS] pressure is lower than { }, the RHR is connected to the primary system to continually remove the decay heat.

13.4.5.18.5 Conclusions

With automatic and manual functions applied in SGTR (1 tube) with VDA [ASDS] stuck open in the SG affected accident, overflow does not occur in the SGa. The source term and radiological consequences are assessed in dub-chapter 13.4.6 and Sub-chapter 13.4.7. It is concluded the acceptance criteria are met in this accident [19].

13.4.6 DEC-A Source Term

The main contribution identified from the DEC-A source terms analysis is fission products in the primary coolant system. From selected DEC-A sequences in Table T-13.4-1, the release path of fission products in the primary coolant system is either discharging to containment by LOCA or leakage to the secondary side by SGTR.

With sequences discharging to containment, such as TLOFW, SBO and SB-LOCA, the release of fission products is bounded by the DBC LOCA in Chapter 12. In the DBC LOCA source term analysis, the gap release resulting from cladding rupture is taken into account and the gravitational settling of aerosols is not considered as part of the conservative assumptions.

With sequences leaking to the secondary side, such as multiple steam generator tubes rupture (10 tubes), main steam line break with SGTR (1 tube) in the affected SG, and SGTR (1 tube) with the VDA [ASDS] stuck open in the SG affected, the release to the environment is larger than for the DBC SGTR source term.

As discussed above, the selected sequences for the DEC-A source term analysis are as listed below:

a) Multiple Steam Generator Tubes Rupture (10 tubes) ;

b) MSLB with SGTR (1 tube) in the affected SG;

c) SGTR (1 tube) with the VDA [ASDS] stuck open in the affected SG.

13.4.6.1 Multiple Steam Generator tubes Rupture (10 tubes)

Multiple SGTR results in radioactive coolant leaking to the secondary side via the ruptured tubes. The leakages of the breaks induce a primary pressure decrease and the contamination of the secondary side. The primary system coolant is considered to be the limit of the technical specification with an iodine spike conservatively. The radioactive coolant discharges to the environment via the VDA [ASDS].

13.4.6.2 MSLB with SGTR (1 tube) in the affected SG

MSLB is located downstream of the MSIV. The SGTR in the affected SG induces uncontrolled discharge of activity to the environment. The release of source terms is terminated once the MSIV is isolated successfully.

13.4.6.3 SGTR (1 tube) with VDA [ASDS] stuck open in the affected SG

SGTR (one tube) leads to the loss of primary coolant, which is transferred to the affected steam generator through the rupture. The VDA [ASDS] being stuck open leads to uncontrolled discharge of activity to the environment until the complete depressurisation of the RCP [RCS] is complete.

13.4.6.4 Method of Analysis

13.4.6.4.1 Calculation inputs

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 the accident. An initial primary coolant activity equivalent to { } is used in the stable state, which is based on the feedback of operating experience.

13.4.6.4.1.2 Thermal Hydraulic Inputs

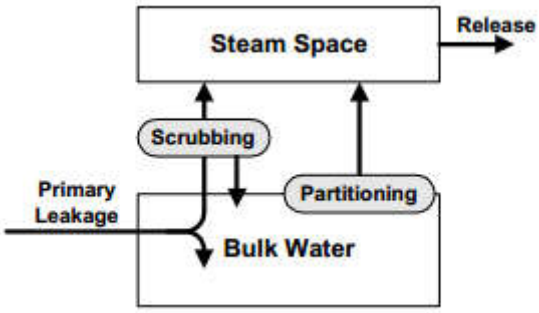
The thermal hydraulic analysis results are given in Sub-chapter 13.4.5, which are taken as the inputs of the DEC-A source term analysis.

13.4.6.4.2 Calculation Models and Assumptions

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.

The transport model of iodine and particulates which are released from the steam generators is shown in Figure F-13.4-1.



F-13.4-1 Source Term Transport Model [20]

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 leak rate limiting condition for the operation.

The break flow rate of the affected SG is determined by the thermal hydraulic results.

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 [20].

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 total tube submergence.

13.4.6.4.2.4 Scrubbing and Partitioning

If the secondary water level is high enough to submerge total tube, the leakage that immediately flashes to vapour will rise through the bulk of the water of the steam generator and enter the steam space.

Scrubbing is credited during periods of total submergence of the tubes. The retention of particulate radionuclides in the steam generator is limited by the moisture carryover (0.25%) from the steam generators [21].

The radioactivity in the bulk water is assumed to become vapour at a rate that is a function of the steaming rate and the partition coefficient. A partition coefficient for elemental iodine of 100 is assumed [20].

13.4.6.5 Results

The results will be presented in PCSR v1.

13.4.7 Radiological Consequences of DEC-A

The evaluation of DEC-A radiological consequences will demonstrate that the requirements of radiation protection targets defined in the generic safety requirements are met [22]. 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

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, the resultant event is termed a Severe Accident (SA) or DEC-B event.

To achieve the safety objectives mentioned in Sub-chapter 13.2, the basic strategy is to maintain the integrity of the containment in both short and long term as far as possible.

However, the integrity of the containment can be challenged by various phenomena and threats occurring 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 HPR1000 (FCG3) and will form the basis of the provisions to be provided for severe accident mitigation in the UK HPR1000 design [23], [24].

13.5.2 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. 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 initiation of an event to lower support plate failure, covering associated phenomena, for instance, core uncovery, core heat-up, core degradation and relocation into lower head.

Initiating with a transient event, 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 and decay heat. With the high temperature of core, the zircaloy oxidation occurs and hydrogen is generated through the metal-water reaction which is highly exothermic and further increases the core temperature. It is noted that the generation of heat from zircaloy oxidation may exceed the decay heat at high temperatures. The fuel as well as control rods and support structures in core regions begins to melt due to the decay heat and oxidation heat of cladding. 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 which are called corium continuously heats up the lower support plate and other support structures, ultimately relocating in the lower plenum after the support plate fails. The relocation path, melting directly downwards through core-support structures to the lower head, is called downward relocation. Another relocation path for the corium is to melt through shroud and barrel then down into the lower head, which is called sideward relocation. The ultimate relocation route into the lower head depends on 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 lower support plate failure to 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 occurs, 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 with rapid energy transfer and the corium particles are generated, which lead to steam generation, shock waves and possible mechanical damage. The phenomenon of this interaction is called in-vessel FCI (in-vessel steam explosion).

The molten corium is solidified during the process of relocation into the lower plenum,

which is called crust. Due to the difference of material densities, the corium pool in the lower plenum consists of two layers:

a) An oxide layer (molten oxide corium with solid crusts surrounded) 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.

The cooling of corium pool in the lower plenum mainly relies on the heat transfer through the gaps between solid crusts and RPV wall. 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 the 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 vessel lower head heat-up. If no additional water is added to the vessel, the corium continues to heat and the RPV lower head failure occurs ultimately.

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, Molten Core-Concrete Interaction (MCCI) and hydrogen combustion.

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 falls into the reactor pit due to the gravity. This may lead to MCCI which however 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 combustion of generated hydrogen during HPME and previous severe accident progression increases the containment pressure as well. This phenomenon 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, 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, thermal degradation and chemical reaction begins, leading to the generation of substantial non-condensable and combustible gas such as H_2 released and accumulated in the containment, raising the risk of containment overpressure and combustible gas combustion and explosion which can seriously threaten the integrity of containment in the long term. If the basemat 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 containment cannot be maintained.

13.5.3 Key Phenomena of Severe Accident 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 Relevant Good Practice (RGP) from a number of sources will be reviewed to determine what 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 these, 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.

Additionally, a matrix will be compiled listing all facilities/operating states within the scope of the GDA and containment states where a severe accident could occur and each phenomenon considered in turn to determine whether it would be appropriate for that facility/operating state/containment state.

13.5.3.1 High Pressure Melt Ejection and DCH

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 mental in the molten corium may oxidized by steam, hydrogen and heat would be produced and 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.

13.5.3.2 Hydrogen Combustion

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 hundreds kilograms of hydrogen could be generated during the in-core process.

If the RPV failed, 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 is mixes with the atmosphere in the containment which and 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 the 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.

13.5.3.3 MCCI

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 may happen to the lower head 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. Complicated physicochemical reactions happen during MCCI. Hence, a large amount of non-condensable gas is produced, leading to an increase of 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 ablated by the melt ceaselessly, which finally leads to radioactive leakage when the concrete pedestal is melted through.

The In-Vessel Retention (IVR) strategy can prevent MCCI by avoiding RPV failure with a high level of confidence according to the demonstration presented in Sub-chapter 13.5.4.3. If the RPV is melted through, the details of the MCCI analysis will be described in the Level 2 PSA report.

13.5.3.4 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.

- In-vessel steam explosion

During severe accidents, in-vessel steam explosion may be possible as the lower head still has water inside it 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 threaten the containment integrity.

According to the SERG-1 Project, SERG-2 Project and SERENA Project, the in-vessel steam explosion is unlikely to occur and the probability of RPV failure caused by an in-vessel steam explosion is very low. The detailed information of these projects is described in References [25] to [29]. Given this consensus of expert opinion on in-vessel steam explosion, it was not considered in the SAA for the HPR1000 (FCG3) and it is supposed to be screened out in the GDA.

- 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.

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 13.5.4.3.

If the 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 occurrence probability. The analysis of ex-vessel steam explosion is given in the Level 2 PSA report.

13.5.3.5 Containment Overpressure

Containment overpressure is one possible containment failure mechanism. During severe accidents, containment pressure increase due to sustained heat from decay power and heat from metal-water reaction can occur. If the RPV is intact, the containment pressure increase is mainly due to steam from the evaporation of the Reactor Coolant System (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.

13.5.3.6 Re-criticality

At the stage of core damage, a problem that may arise from water injection is 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, but the stack of fuel elements is still largely intact, as a consequence of the injection of water that is not borated, or at least adequately borated, there might be regions of the core without control rods which may result in core re-criticality. In principle, power could increase to the amount that corresponds to evaporation of all water injected. Power peaks are possible if the feedback mechanisms of reactivity addition are not fast enough.

For UK HPR1000, the re-criticality during in-vessel recovery is unlikely to occur for the following reasons.

- In the early stage after the start of an accident, because a large degree of the melting of control rods would not have occurred, re-criticality will not occur even if the unborated water is injected into the core.

- 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 increases in this stage. However,

according to the analysis of severe accident sequences, this stage is very short and the probability of recovering core cooling using unborated water in this short interval is significantly small.

- For UK HPR1000, according to the strategy of injecting water into the primary system, borated water source is preferred. If boron injection is conducted, the re-criticality event does not occur. Even if unborated water may be injected in some cases, before unborated water source is injected into the core, an assessment of the negative effects will be performed based on severe accident management strategy firstly, and it should be ensured that the core does not have a re-criticality risk.

From the above considerations, it is judged that the risk of re-criticality during in-vessel recovery is limited for the UK HPR1000. Detailed analysis on the phenomenon will be performed to determine if it is reasonable to exclude re-criticality from UK HPR1000.

13.5.4 Descriptions of Severe Accident Mitigation Measures

To avoid an early or large release of radioactive substances in DEC-B conditions, the mitigation measures are designed to prevent early failure of the containment and ensure the long-term integrity of the containment. 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 reduce the 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 is designed to maintain the corium within the RPV and consequently preserve the integrity of the containment, thus preventing ex-vessel steam explosion, MCCI and DCH;

e) EUF [CFES] to prevent containment overpressure as the ultimate way 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 GDA process of UK HPR1000, the qualification specifications of equipment will be provided in GDA process. 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.

13.5.4.1 SADV

13.5.4.1.1 Safety Functions

A failure of the RPV under high internal pressure is of importance to severe accident risk as missiles could be created from vessel movement. HPME could lead to DCH by melt debris dispersed inside the containment atmosphere, which could result in subsequent containment failure. Therefore, the ability to reduce the primary pressure, under severe accidents with high pressure, should be ensured so that high pressure core melt situations can be avoided. In the design of the UK HPR1000, the dedicated Severe Accident Depressurisation Valves (SADVs) are specially designed for primary depressurisation under severe accidents and can realise the following safety functions:

a) To be opened when required and remain open 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.

13.5.4.1.2 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] is lower than 2.0 MPa abs. before RPV failure [30], in order to avoid a high-pressure core melt accident. The discharge capacity of one SADV line is 630 t/h at 17.23 MPa abs. under saturated steam conditions.

13.5.4.1.3 Mitigation Measures

The ability to reduce the primary pressure under severe accidents with high pressure is achieved through SADVs on two discharge lines on top of the pressuriser. Each line includes two valves in series that are connected to the same pressuriser nozzle, located at the same elevation as the nozzles of the pressuriser safety valves (PSVs). Both the SADVs and PSVs are connected to the line that ends in the pressuriser relief tank.

The criterion for opening the dedicated SADVs is that the SADVs are opened manually for primary depressurisation when the core outlet temperature reaches 650°C.

The implementation and discharge capacity of the SADVs provide time margin for the operator’s depressurisation operation under severe accidents. Even in the case of LOOP and failure of all emergency diesels, the SADVs should be able to be opened when required and remain open, otherwise they should be able to remain closed – not

leak or fail – until they are opened by the operator.

13.5.4.2 EUH [CCGCS]

Under severe accidents, a large amount of hydrogen releases into the containment. The mixtures of hydrogen and air may burn when the hydrogen concentration exceeds 4 vol%. If the hydrogen concentration exceeds 10 vol%, hydrogen detonation is likely to occur. Hydrogen detonation can form powerful shock waves and challenge the containment integrity. In order to deal with containment failure risk due to hydrogen combustion in the containment, the EUH [CCGCS] is arranged in the UK HPR1000.

13.5.4.2.1 Safety Functions

The EUH [CCGCS] for the UK HPR1000 includes two sub-systems:

a) Passive Autocatalytic Recombiners (PARs) sub-system;

b) Hydrogen monitoring sub-system.

Main safety functions of the EUH [CCGCS] are as follows:

a) Limiting and reducing local hydrogen accumulation and containment failure risks caused by hydrogen combustion;

b) Limiting the average hydrogen concentration in the containment to be below 10 vol % under severe accidents. The purpose is to reduce containment failure risk caused by hydrogen combustion;

c) Maintaining the containment integrity during severe accidents.

13.5.4.2.2 Design Basis

The design of the EUH [CCGCS] for the UK HPR1000 must meet the following requirements:

a) Hydrogen concentration must be limited in the containment during and following severe accident conditions, uniformly distributed, to be less than 10 vol%;

b) Following severe accident conditions, if local hydrogen flame acceleration occurs, the integrity of the containment should be maintained.

The design objective of the EUH [CCGCS] is to reduce the hydrogen concentration in the containment during severe accidents and design basis accidents such as LOCA. The EUH [CCGCS] is not running under normal operation conditions, but can start up automatically in a hydrogen/steam atmosphere following the design basis accidents and severe accidents.

13.5.4.2.3 Mitigation Measures

Hydrogen is light gas which tends to flow upward after its generation. The containment for the UK HPR1000 is a one-room structure which is good for natural

convection ensuring homogeneous mixing and avoids hydrogen building-up in dead-spaces. The steam released from the primary break or SADV helps to mix and dilute the combustible mixtures.

The EUH [CCGCS] consisting of hydrogen recombiners and a hydrogen monitoring sub-system is designed and facilitated in the containment to mitigate the hydrogen risks. A total number of 29 passive autocatalytic recombiners are equipped in the containment in locations which are good for natural convection. These recombiners consist of several catalyst plates at their inlets, which will help the reaction of hydrogen by the principle of the catalytic chemical process. By this principle, the passive autocatalytic recombiners are capable of working when the hydrogen concentration reaches 2 vol%. In addition, 10 hydrogen sensors are located in the representative locations in the containment to indicated the hydrogen risk in concert with the pressure measured in the containment. Information on the technology used to perform hydrogen monitoring is described in PCSR Chapter 7.

13.5.4.3 IVR

13.5.4.3.1 Safety Functions

After a severe accident, the core may melt due to insufficient cooling. The corium will relocate into the lower head of the RPV. Due to the temperature of the corium being 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 the cooling water can 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 removes heat from the corium pool. Therefore the IVR strategy can prevent RPV failure, avoiding many ex-vessel phenomena (DCH, steam explosion and MCCI) which may threaten the containment integrity.

13.5.4.3.2 Design Basis

In order to retain the corium inside the RPV after severe accidents, the following two success criteria need to be met:

a) After the corium relocates into the lower head, the heat flux conducted through the wall of the RPV has to be lower than the local Critical Heat Flux (CHF);

b) After the relocation of corium, the wall of the RPV becomes thinner due to melting by corium in the lower head. The minimum thickness of the wall must have enough mechanical strength to maintain the integrity of the RPV.

The IVR strategy is one of the important severe accident mitigation measures for UK

HPR1000, and 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 affecting nuclear power plant safety 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.

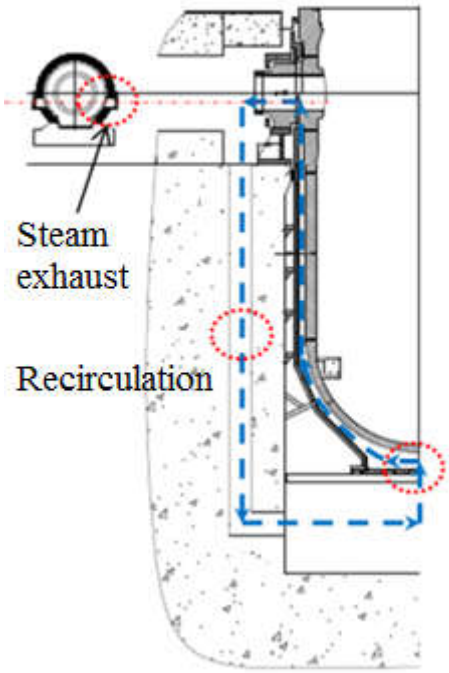
13.5.4.3.3 Mitigation Measures

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 IVR tank while active IVR injects water from IRWST.

When 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 already been justified by the bounding severe accidents sequence (Large Break Loss of Coolant Accident).

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 in different compartments than the SADV discharge line. The opening of the SADV has little effects on the reliance of the reactor pit flooding system valves.

To ensure the effectiveness of the IVR strategy, an RPV insulation layer is especially 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-13.5-1 Sketch design of flow channel

13.5.4.4 EHR [CHRS]

13.5.4.4.1 Safety Functions

Due to steam and non-condensable gas accumulation in severe accidents, in the case of no any other mitigation measures, the containment pressure increases slowly and constantly. Finally, the containment pressure reaches the containment failure pressure, thus leading to containment failure in the long term. For long-term containment heat removal, the UK HPR1000 has a dedicated EHR [CHRS] which is specially designed for containment heat removal to avoid containment overpressure failure 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 Sub-chapter mainly describes the spray mode of the EHR [CHRS] which implements the containment heat removal function. In the following context the EHR [CHRS] only refers to the containment spray sub-system. The details of IVR strategy, including passive reactor pit water injection and active reactor pit water injection, are introduced in Sub-chapter 13.5.4.3.

The safety functions of the EHR [CHRS] are as follows:

a) Transferring the heat of the containment atmosphere to the IRWST;

b) Transferring the heat of the IRWST to the UHS.

13.5.4.4.2 Design Basis

The objective of the EHR [CHRS] is to control containment pressure under severe accident conditions and conduct long-term cooling on the containment atmosphere and IRWST. Moreover, after severe accidents, the containment can provide a 12-hour operator non-intervention grace period. During this time, the pressure in the containment can be kept lower than the design pressure without any operator action required. After the 12-hour grace period, the actuation of the EHR [CHRS] can remove the containment heat to avoid containment overpressure failure. To realise this objective, the following success criteria 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.

b) Long-term function criteria

During the long-term operation of the EHR [CHRS], one train of the EHR [CHRS] assures that the pressure of the containment is maintained below { }.

13.5.4.4.3 Mitigation Measures

The containment spray sub-system of the EHR [CHRS] has two identical trains physically isolated. The essential components (for each main train) are a dedicated suction line from the IRWST, spray rings and nozzles, an EHR [CHRS] pump, a heat exchanger, three discharge lines (for spray, reactor pit injection and sump screen back wash), a pipe connecting the EHR [CHRS] pump inlet and adjacent safety injection system (RIS [SIS]) pump inlets. For the details of the EHR [CHRS] design refer to PCSR Sub-chapter 7.4.2.

Within the 12-hour grace period of severe accidents, even when the containment spray of the EHR [CHRS] is not started, the pressure and temperature in the containment can be maintained below the design limits. After the 12-hour grace period of severe accidents, the operator starts the spray manually based on the containment pressure.

13.5.4.5 EUF [CFES]

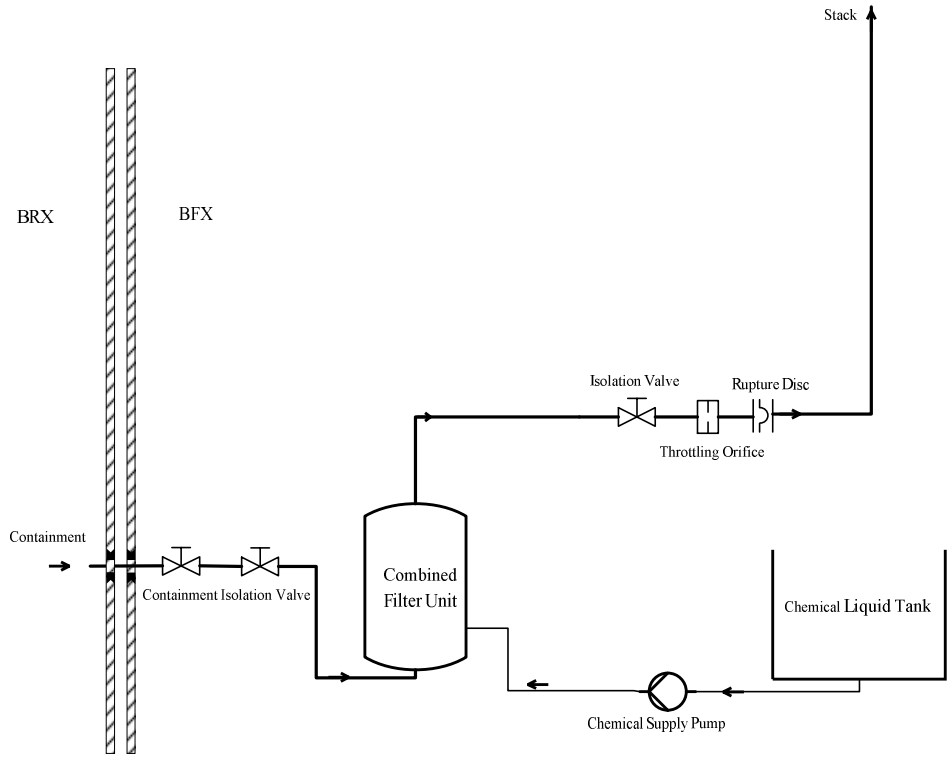
The design of the EUF [CFES] is based on the HPR1000 (FCG3) and may change in the UK HPR1000 according to further research.

13.5.4.5.1 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 in case the containment spray of EHR [CHRS] is unavailable.

The EUF [CFES] controls containment pressure by venting and filtering containment atmosphere to the environment. The description of EUF [CFES] system and main equipment can be found in Sub-chapter 7.4.3.4. The decontamination factors of aerosol, element iodine and organic iodine are 1000, 100 and 5, respectively.



F-13.5-2 Schematic Diagram of the EUF [CFES]

13.5.4.5.2 Design Basis

When the EUF [CFES] is opened, containment pressure keeps sustained decrease. The release of radioactive substances is acceptable and as low as possible.

13.5.4.5.3 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 applied for operation. However, the approval to open the EUF [CFES] is decided by the emergency organisation.

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 manual local opening or closing of the isolation valve, 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.

13.5.5 Selection of Representative DEC-B Events

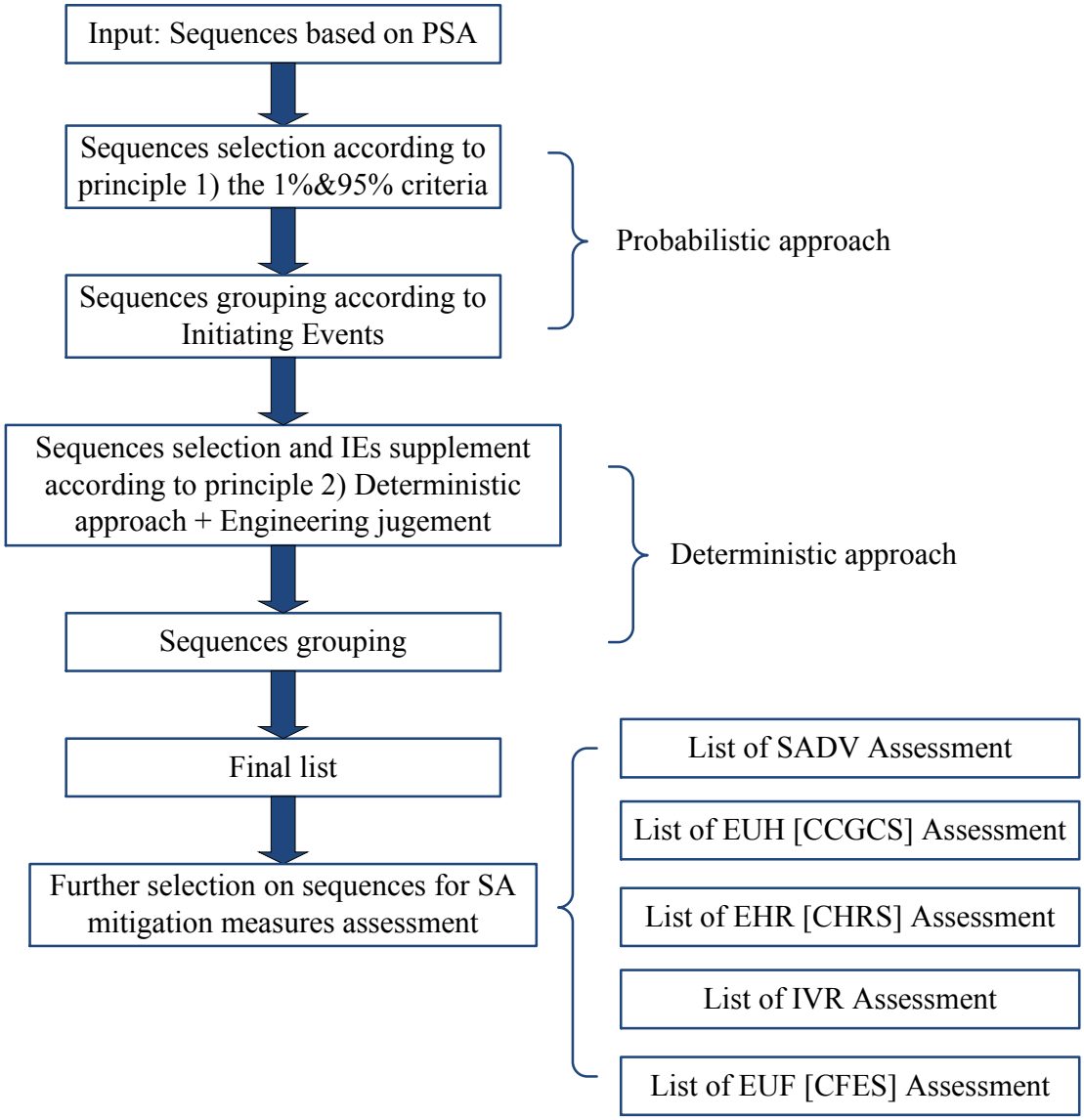
13.5.5.1 Principles and Methods

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 [31].

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 Figure F-13.5-3 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 differences of different system objectives to ensure the selected sequences are the bounding ones.



F-13.5-3 Process of severe accident sequence selection

13.5.5.2 Severe Accident Sequences List Identification

In this section, the representative severe accident sequences of the UK HPR1000 are selected based on the Level 1 PSA results of the HPR1000 (FCG3) since the PSA work for UK HPR1000 is still ongoing. The list will be updated when the Level 1 PSA results for the UK HPR1000 are ready. The selection method combines the probabilistic and deterministic methods with rational engineering judgements.

13.5.5.2.1 Selection Based on Probabilistic Method

13.5.5.2.1.1 Selection based on First Principle

According to the first selection principle in Sub-chapter 13.5.5.1, the Level 1 PSA results of the HPR1000 (FCG3) were analysed to determine the domain sequences. All operating states such as at-power, low power and shutdown as shown in Table

T-13.5-1 were analysed by the HPR1000 (FCG3) Level 1 PSA. All the sequences of which the total sequence exceeds 95% of the total CDF were screened in the severe accident the sequence list. It is shown that this list covers not only all the sequences for which sequence exceeds 1% of the total CDF but also some of the sequences for which the sequence is less than 1% of the total CDF.

13.5.5.2.1.2 Preliminary grouping from PSA perspective

In Sub-chapter 13.5.5.2.1.1, 46 severe accident sequences are selected preliminarily based on the probabilistic method, wherein, 15 of them are at power condition, while 31 of them are at shutdown condition. This list should be grouped according to initiating events and system functions. For grouping, the following criteria are used: 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, and these two sequences could be grouped. In the HPR1000 (FCG3), the 46 accident sequences selected were grouped into 12 types including 37 sequences as shown in Table T-13.5-2.

13.5.5.2.2 Selection Based on Deterministic and Engineering Judgements

According to the second selection principle in Sub-chapter 13.5.5.1, 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 Level 1 PSA initiating events, sequences of loss of main feedwater in POSA, LOOP in POSA, Interfacing Systems Loss of Coolant Accident (ISLOCA), cold overpressure and Large Break Loss of Coolant Accident (LB-LOCA) are screened out because of the low frequencies. However, the sequences of LB-LOCA, 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 the accident sequence with the same or similar progress, the one with higher consequence bounds the lower ones.

The severe accident of 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 sequences of loss of feedwater in POS B, the similar sequence of loss of heat sink 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 D based on the deterministic analysis and engineering judgements .

The progression of loss of residual heat removal, LOOP and loss of heat sink in POS E/G are similar, so they are grouped into loss of residual heat removal in POS G in which the water inventory is less than for POS E.

The ATWS sequences selected from the PSA are considered as core damage conservatively in the Level 1 PSA model. Therefore, ATWS category sequences with availability of RBS and loss of secondary side cooling are selected by engineering judgements instead.

For the boron dilution events in POS E, SLB with ATWS, they are also conservative consideration in PSA model. Therefor they are screed 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 screed out of the list.

Through the above analysis, the final list of severe accidents after grouping includes 7 categories and 10 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. The fuel melt sequences in the SFP will be supplemented according to the SFP PSA of the UK HPR1000.

13.5.5.2.3 Accident Sequence Selection for Different Mitigation Measures Assessment

For the assessment of severe accident mitigation measures, the bounding accident sequences are selected starting from Table T-13.5-3. Conservative assumptions are adopted for different analysis objectives because of different severe accident phenomenon and progression. For the assessment of different severe accident mitigation measures, the bounding sequences are selected as shown in Table T-13.5-4. The selection principle and process is described in detail in the following Sub-chapters.

13.5.5.2.3.1 Bounding sequences selection for the assessment of SADV

The SADV is designed to prevent containment over-heating and overpressure caused by high-pressure melt ejection. For the assessment of the SADV, sequences with high primary pressure are selected. According to the deterministic and engineering judgements, ATWS, SBO, etc. are usually selected as shown in Table T-13.5-4.

13.5.5.2.3.2 Bounding sequences selection for the assessment of EUH [CCGCS]

The EUH [CCGCS] is designed to reduce the risk from combustion and explosion.

From the perspective of the hydrogen risk, the hydrogen generation rate, the total mass of hydrogen generated and the total mass of water vapour generated are all factors that will affect the hydrogen risk. A high hydrogen generation rate often induces high local hydrogen concentrations and hydrogen risk. The mass of water vapour has two-side effects: a decreasing water vapour generation rate often induces a relatively higher hydrogen concentration; on the other hand, a decreasing water vapour generation rate will reduce the AICC pressure.

For the assessment of the EUH [CCGCS], LB-LOCA is selected because of the generation of large amount of water vapour. In addition, SB-LOCA, Intermediate Break Loss of Coolant Accident (IB-LOCA) and SBO are also analysed to study the hydrogen source because of their slower accident progress, possible larger amount of hydrogen production and the different hydrogen release locations.

13.5.5.2.3.3 Bounding sequences selection for the assessment of EHR [CHRS]

The EHR [CHRS] is designed to prevent containment overpressure failure. For the assessment of the EHR [CHRS], sequences with a fast and massive mass energy release in the containment which could lead to the containment pressure increasing are selected. If more mass and energy is released to the containment, the challenges to the containment increase. According to the deterministic assessment and engineering judgment, LB-LOCA is the fast release situation therefore LB-LOCA is usually selected as is shown in T-13.5-4.

13.5.5.2.3.4 Bounding sequences selection for the assessment of IVR

The IVR strategy uses external RPV cooling to maintain the corium inside the RPV. For the assessment of the IVR, the accident sequences challenging the RPV with fast and massive relocation of molten corium shall be selected as the bounding sequences. Typically, those sequences are LB-LOCA without availability of active safety injections which leads to a complete uncovering of the core and relocation of corium quickly after core uncovery. LB-LOCA is selected as the bounding sequence, and also IB-LOCA, SB-LOCA, SBO and ATWS sequences are selected for the uncertainty analysis as shown in Table T-13.5-4.

13.5.5.2.3.5 Bounding sequences selection for the assessment of EUF [CFES]

The EUF [CFES] is designed to prevent containment overpressure and limit the release of airborne radioactivity at the site boundary within acceptable levels. For the assessment of the EUF [CFES], the accident sequence that may lead to containment overpressure shall be selected. According to the deterministic assessment and engineering judgement, LB-LOCA is usually selected as shown in Table T-13.5-4 because of its early release and fast progression.

T-13.5-1 Plant Operating States Analysed in HPR1000 (FCG3) PSA

POS	Name	Operation mode	Descriptions
POS A	Power operation	RP	POS A includes full power operation, low power and hot standby state (analysed as full power operation state).
POS B	Shutdown condition of SG cooling mode	NS/SG	POS B includes shutdown operation state through SG cooling before the residual heat removal is connected.
POS C	Shutdown condition of RHR cooling mode	NS/RIS -RHR	POS C includes shutdown operation state through SG cooling after the residual heat removal is connected.
POS D	Maintenance of cold shutdown with manhole closed	MCS	POS D includes the maintenance of cold shutdown, RCP [RCS] is non-closed but able to be pressurized.
POS E	Maintenance of cold shutdown with manhole opened	MCS	POS E includes the maintenance of cold shutdown, RCP [RCS] is non-closed and not able to be pressurised.
POS G	MID-LOOP condition	---	This is the special operation state possible under MCS mode. Since there is certain risk because of low primary water level, it shall be separately divided and treated.

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 not implemented in time, MHSI failed to be put into operation, and core damage
		POS A, SB-LOCA, MHSI failure, failed to enter the low pressure full cooldown, and core damage
		POS B, SB-LOCA, MHSI failure, low pressure full cooldown failure, and core damage
		POS E, SB-LOCA, IRWST cooling failure, and core damage
2	SGTR	POS A, single-tube SGTR, secondary cooling failure, feed and bleed not implemented in time, MHSI failed to be put into operation, and core damage
		POS A, single-tube SGTR, MHSI failure, failed to enter the low pressure full cooldown, and core damage
		POS B, single-tube SGTR, MHSI failed to be put into operation, low pressure full cooldown failed to be implemented, LHSI failed to be put into operation in time, and core damage
		POS A, single-tube SGTR, medium pressure rapid cooldown failure, feed and bleed not implemented in time, MHSI failed to be put into operation, and core damage

SN	Category	Sequence description
3	ATWS	POS A, loss of main feedwater plus reactor trip failure, KDS [DAS] signal not sent correctly, and core damage
		POS A, loss of main feedwater plus reactor trip failure, reactor coolant pump failed to trip, and core damage
		POS A, single-tube SGTR, control rod stuck (more than 3), reactor shutdown failure, and core damage (conservative consideration)
		POS B, main steam pipeline break, reactor trip failure and core damage
4	Loss of heat sink	POS A, loss of heat sink, secondary cooling failure, feed and bleed not implemented in time, MHSI failed to be put into operation, and core damage
		POS E, loss of heat sink, water supply failure of LHSI system, core being damaged after the water is vaporised to dry
		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

SN	Category	Sequence description
6	SLB + SGTR	POS A, SLB with SGTR accident, being unable to cool to the RIS [SIS] connection state, and core damage (primary continuous high pressure, being unable to effectively isolate the damaged SG, possible bypass to the containment)
7	IB-LOCA	POS A, IB-LOCA, RIS accumulator failure, and core damage
		POS A, IB-LOCA, failure of LHSI to the cold leg and hot leg simultaneously, and core damage
		POS C, IB-LOCA, MHSI failure, and core damage
		POS B, IB-LOCA, failure of LHSI to the cold leg and hot leg simultaneously, and core damage
8	Loss of residual heat removal	POS E, loss of residual heat removal, MHSI failure, core being damaged after the water is vaporised to dry
		POS E, loss of residual heat removal system, IRWST cooling failure, and core damage
		POS C, loss of residual heat removal function accident, secondary cooling failure, feed and bleed failure, and core damage
		POS G, loss of residual heat removal function, MHSI failure

SN	Category	Sequence description
		POS G, loss of residual heat removal system, IRWST cooling failure, and core damage
		POS D, loss of residual heat removal function, secondary cooling failure, feed and bleed operation not implemented in time, and core damage
9	LOOP	POS E LOOP, EDG and SBO DG failed to be started, and core damage
		POS C LOOP, EDG and SBO DG failed to be started, and core damage
		POS E, LOOP, RHR failure, water supply failure of MHSI, and core damage
		POS D, LOOP, EDG and SBO DG failed to be started, and core damage
		POS G, LOOP, EDG and SBO DG failed to be started, and core damage
		POS G, LOOP, RHR failure, water supply failure of MHSI, and core damage
10	Loss of feedwater	POSB, loss of startup and shutdown feedwater system, secondary cooling failure, feed and bleed operation not implemented in time, and core damage

SN	Category	Sequence description
11	Boron dilution	POSE, boron dilution, failed to isolate dilution sources automatically and failure for operator manual isolation
12	SLB	POSB, SLB, secondary cooling failure, 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. The same SGTR sequence is bounded
		POS A, SB-LOCA, MHSI failure, failed to enter the low pressure full cooldown, and core damage	Based on the sequence selected by the PSA, merging POS A and POS B, and enveloping the two with POS A. The same SGTR sequence is bounded. The similar sequence in POS E is also bounded.

SN	Category	Sequence after merging	Description
2	LB-LOCA	POS A, LB-LOCA, MHSI and LHSI failure and core damage	Supplementation based on deterministic and engineering judgement
3	IB-LOCA	POS A, IB-LOCA, RIS accumulator failure, and core damage	From PSA
		POS A, IB-LOCA, failure of LHSI, and core damage	Based on the sequence selected by the PSA, merging POS A and POS B, and enveloping the two with POS A. Failure of LHSI to the cold leg and hot leg simultaneously is instead of failure of LHSI from the deterministic perspective.
		POS A, IB-LOCA, MHSI failure, and core damage	From deterministic perspective, bounding the similar sequence in POS C from PSA

SN	Category	Sequence after merging	Description
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	Supplementation based on deterministic and engineering judgement
5	Loss of feedwater	POS A, total loss of feedwater, feed and bleed operation not implemented in time, and core damage	From deterministic perspective and as the similar sequence in POS B from PSA can be bounded. The similar sequence of loss of heat sink from the PSA can be bounded. Loss of residual heat removal in POS C from the PSA can be bounded.

SN	Category	Sequence after merging	Description
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, D.
7	Loss of residual heat removal	POS G, loss of residual heat removal, MHSI failure, and core damage.	Based on the sequence selected by the PSA, merging POS E and POS G (which is a mid-loop condition and can envelop POS E) Besides, under such conditions, the sequence of core damage caused by MHSI failure after loss of residual heat removal function can envelope the sequences of IRWST cooling failure. Loss of heat sink and loss of offsite power in the same POS can be bounded.

T-13.5-4 Accident Sequence Selected for the Different Severe Accident Mitigation Measures Assessment

SN	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

SN	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

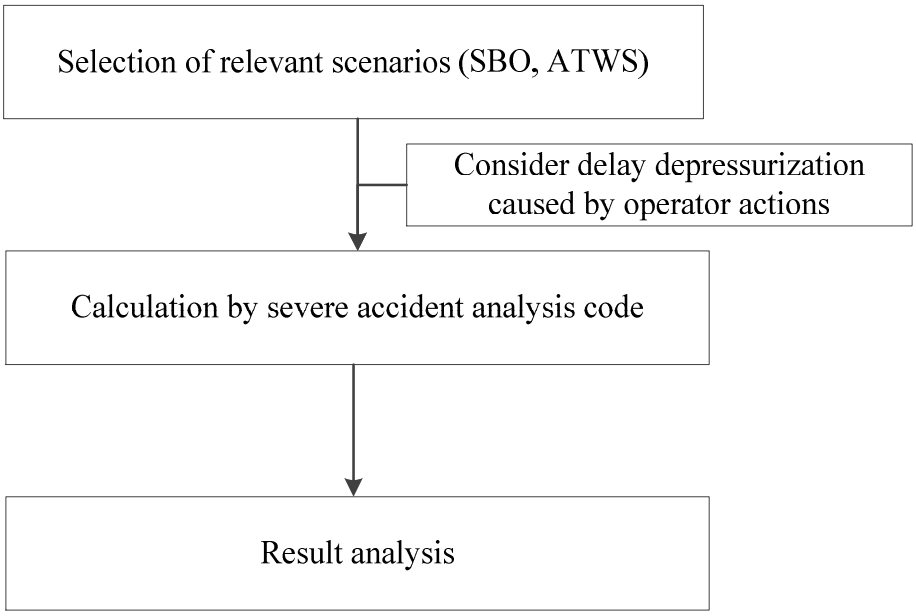
13.5.6 Assessment of SA Mitigation Measures

Based on the selection process in Sub-chapter 13.5.5, the DEC-B sequences listed in Table T-13.5-4 are analysed based on best estimate assumptions to demonstrate that the mitigation measures are effective.

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 as follows:



F-13.5-4 The flow-chart of SADV effectiveness analysis

a) Selection of relevant scenarios

The design target of SADVs is to transfer high pressure core melt scenarios to low pressure core melt scenarios with high reliability, so that high pressure core melt situations can be prevented. For the assessment of the SADV, it is reasonable to select the sequences with high primary pressure to verify whether the discharge capability of SADVs is sufficient for primary depressurisation. According to the deterministic assessment and engineering judgement, ATWS and SBO are selected to be analysed. The delay to depressurisation caused by operator actions should also be taken into consideration.

b) Calculate by integral severe accident analysis code

Calculations are performed by using ASTEC code, and the description of the code has

been given in Appendix 13A. The accident assumptions are shown in Sub-chapter 13.5.6.1.2.

c) Result analysis

After the calculations, the two sequences (SBO, ATWS) curves of primary pressure, primary average temperature, containment pressure and depressurisation flow rate of SADVs are obtained.

13.5.6.1.2 Event Description

As described above, SBO and ATWS sequences should be analysed, 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 can't be removed in a timely manner from the core if secondary cooling fails, which leads to an increase of primary pressure. The PSVs open automatically when primary pressure increases to its threshold value, which results in a loss of primary coolant. Subsequently, the core is uncovered. When the core outlet temperature reaches 650°C, the SADVs are opened manually for primary depressurisation.

The initial conditions for the accident analysis are as follows:

a) The initial reactor operation at the 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 accumulator available;

e) MHSI unavailable;

f) LHSI unavailable;

g) Containment spray system unavailable;

h) Opening of the SADVs when core outlet temperature exceeds 650 °C;

i) The PSVs are closed when the SADVs are opened for conservative consideration.

13.5.6.1.2.2 SBO + delayed depressurisation

For this scenario, compared to the SBO described above, the opening time of SADVs

is delayed by 0.5h after the core outlet temperature reaches 650°C.

The initial conditions for the accident analysis are as follows:

a) The initial reactor operation at the 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 accumulator available;

e) MHSI unavailable;

f) LHSI unavailable;

g) Containment spray system unavailable;

h) The time for delaying depressurisation is 1800 s;

i) The PSVs are closed when the SADVs are opened for conservative consideration.

13.5.6.1.2.3 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. This leads to a primary temperature and pressure rise. The PSVs open automatically when the primary pressure increases to its threshold value, which results in a loss of primary coolant. Subsequently, the core is uncovered. When the core outlet temperature reaches 650°C, the SADVs are opened manually for primary depressurisation.

The initial conditions for the accident analysis are as follows:

a) The initial reactor operation at the full power condition;

b) The sequence is initiated by loss of the main feedwater and reactor trip fails.

The related assumptions for the accident analysis are as follows:

a) ASG [EFWS] unavailable;

b) RIS accumulator available;

c) MHSI unavailable;

d) LHSI unavailable;

e) Containment spray system unavailable;

f) Opening of the SADVs when core outlet temperature exceeds 650 °C;

g) The PSVs are closed when the SADVs are opened for conservative consideration.

13.5.6.1.2.4 ATWS + delayed depressurisation

For this scenario, compared to the ATWS described above, the opening time of the SADVs is delayed by 0.5h after the core outlet temperature reaches 650°C.

The initial conditions for the accident analysis are as follows:

a) The initial reactor operation at the full power condition;

b) The sequence is initiated by loss of the main feedwater and reactor trip fails.

The related assumptions for accident analysis are as follows:

a) ASG [EFWS] unavailable;

b) RIS accumulator available;

c) MHSI unavailable;

d) LHSI unavailable;

e) Containment spray system unavailable;

f) The time for delaying depressurisation is 1800 s;

g) The PSVs are closed when the SADVs are opened for conservative consideration.

13.5.6.1.3 Effectiveness evaluation of SADV

In this section, six cases are calculated with using ASTEC code to evaluate the effectiveness of the SADV. The description of the code has been given in Appendix 13A.

13.5.6.1.3.1 SBO

a) Without SADV

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.

b) With SADV

For this scenario, the SADV be opened when core outlet temperature exceeds 650 °C, and the primary pressure drops quickly after the SADV be opened.

13.5.6.1.3.2 SBO + delayed depressurisation

For this scenario, the opening time of SADVs is delayed by 0.5h after the core outlet temperature reaches 650°C, and the primary pressure drops quickly after the SADV be opened.

13.5.6.1.3.3 ATWS

a) Without SADV

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.

b) With SADV

For this scenario, the SADV be opened when core outlet temperature exceeds 650 °C, and the primary pressure drops quickly after the SADV be opened.

13.5.6.1.3.4 ATWS + delayed depressurisation

For this scenario, the opening time of SADVs is delayed by 0.5h after the core outlet temperature reaches 650°C, and the primary pressure drops quickly after the SADV be opened.

13.5.6.1.4 Conclusion

As the dedicated measures for the severe accident mitigation, the SADVs are designed to convert high pressure core melt scenarios into low pressure scenarios with a high reliability.

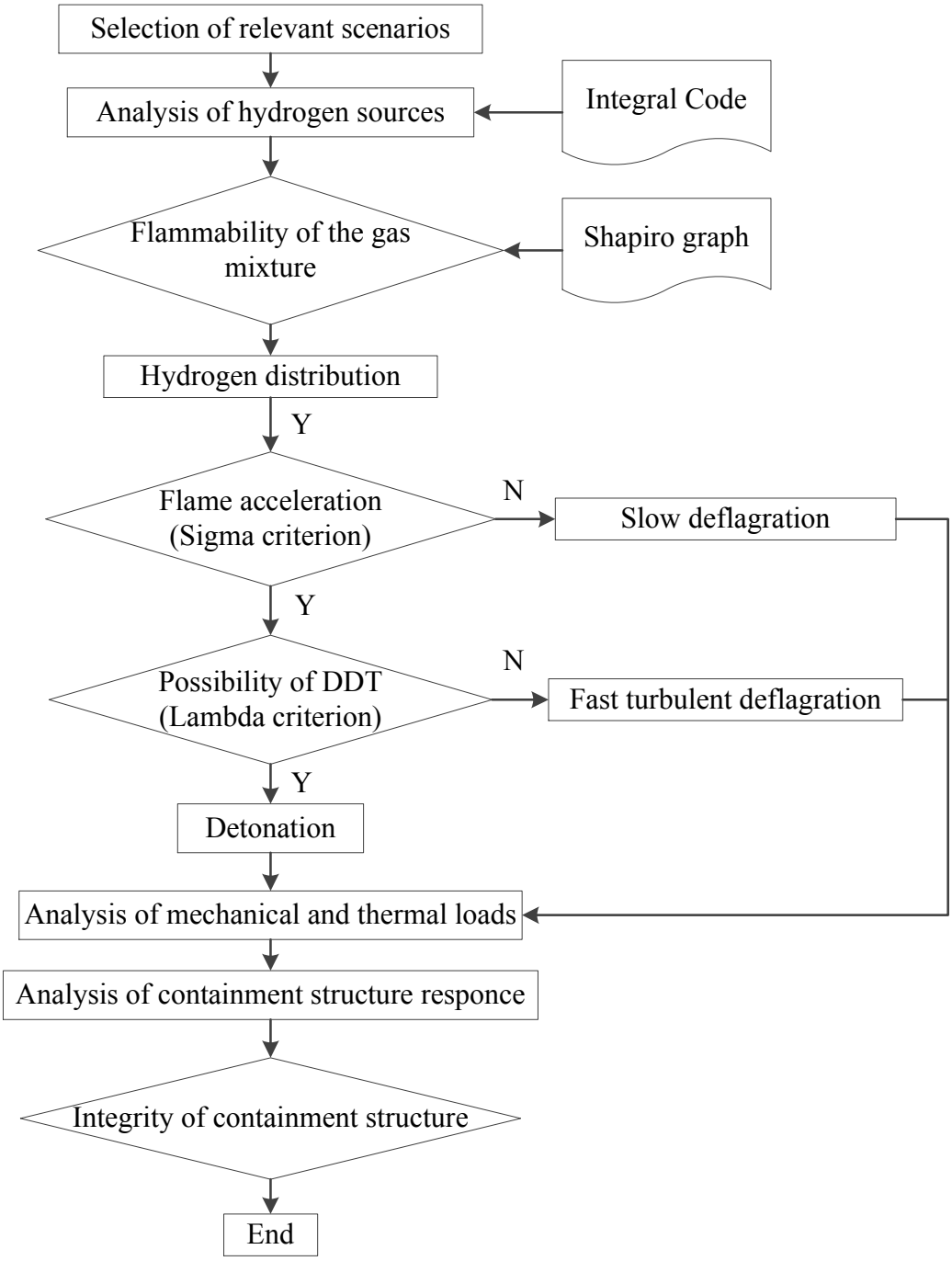
The calculation on assessment of SADV for reference design, HPR1000 (FCG3), has been finished. The conclusion is that the discharge capacity of the SADVs is sufficient to meet the design basis.

For UK HPR1000, based on the ASTEC calculation results of SBO sequence, the design of SADVs can meet the design basis and effectively eliminate the risk of high pressure core melt, and the detailed results and conclusions are supplemented in supporting documents [32] during Step 3. The calculation results of ATWS sequence will be supplemented in PCSR v1 at the entry of Step 4.

13.5.6.2 Assessment of the EUH [CCGCS]

13.5.6.2.1 Method for the Assessment of the EUH [CCGCS]

Several steps are taken to assess the EUH [CCGCS] and hydrogen risk, the analysis flow-chart is as follows:



F-13.5-5 Flow-chart of the EUH [CCGCS] assessment

a) According to the PSA results and engineering judgements, a set of relevant accident sequences are selected to demonstrate the adequacy of the EUH [CCGCS]. In the HPR1000 (FCG3), the initiating events of SB-LOCA, IB-LOCA, LB-LOCA and SBO are analysed. LOCAs with different break sizes will lead to different hydrogen production characteristics, while SBOs progress slowly and usually get larger amounts of hydrogen.

b) Evaluation of the gas sources for the postulated severe accidents. This step will be performed for various of accident scenarios using ASTEC.

c) Evaluation of the flammability of the gases and gas distribution. A Shapiro graph can be used as a simple tool to assess the flammability of gases.

d) Assessment of the possibility of flame acceleration and DDT. The sigma and lambda criteria are used to assess the possibility of flame acceleration and DDT in specific zones. As the local distribution is critical for the flame transmission, more sophisticated Computational Fluid Dynamics (CFD) codes such as GASFLOW are applied.

e) Determination of the thermal loads of the combustion process including slow deflagration, fast deflagration or detonation on structures.

f) If fast combustion modes cannot be excluded, the pressure load will be investigated in detail. In the analysis for the HPR1000 (FCG3), hydrogen explosion can be excluded and the fast combustion that is possible to occur will not threaten the integrity of the containment.

13.5.6.2.2 Event Description

As described above, a set of relevant accident sequences should be analysed to assess the effectiveness of the EUH [CCGCS]. Accident sequences selected for the effectiveness of the EUH [CCGCS] include LB-LOCA, IB-LOCA, SB-LOCA and SBO.

Hydrogen generation through MCCI is slow and it can be reduced effectively by the passive autocatalytic recombiners. For the analysis of the UK HPR1000, it is assumed that the IVR strategy is available. The hydrogen generation considered is from the core.

13.5.6.2.2.1 LB-LOCA

In LB-LOCA, a large amount of coolant discharges from the break and the containment pressure increases quickly due to large amount of vapour injection. The accident progress is very fast. When the RCP [RCS] pressure is lower than injection threshold value, the RIS accumulators begin to inject water into the RCP [RCS]. However, due to the failure of the safety injection and the secondary side, the coolant inventory in the RPV cannot be maintained and core uncovery occurs. Hydrogen is generated by the zirconium-water vapour reaction when the clad temperature exceeds threshold values.

The initial conditions for LB-LOCA are as follows:

a) Initial reactor operation at state A;

b) Large break of diameter 30 cm (706.5 cm^2) occurs in the cold leg.

The assumptions for LB-LOCA are as follows:

a) RIS accumulator available;

b) MHSI unavailable;

c) LHSI unavailable;

d) Containment spray system unavailable;

e) IVR available;

f) Opening of the SADV when maximum core outlet gas temperature exceeds 650 °C.

13.5.6.2.2.2 IB-LOCA

In IB-LOCA, the coolant discharges from the break into the containment when the accident occurs. Because of the failure of safety injections, the core uncovery occurs and core temperature increases. A large amount of hydrogen is generated by the zirconium-water vapour reaction when the cladding temperature exceeds threshold values.

The initial conditions for IB-LOCA are as follows:

a) Initial reactor operation 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 as follows:

a) RIS accumulator available;

b) MHSI unavailable;

c) LHSI unavailable;

d) Containment spray system unavailable;

e) IVR available;

f) Opening of the SADV when maximum core outlet gas temperature exceeds 650 °C.

13.5.6.2.2.3 SB-LOCA

In SB-LOCA, the coolant discharges from the break into the containment when the accident occurs. Because of the failure of safety injections, the core uncovery occurs and core temperature increases. When the core outlet temperature reaches 650 °C, the SADV is opened manually for primary depressurization. Cladding temperature increases quickly and hydrogen is produced by the reaction of zirconium and vapour.

The initial conditions for SB-LOCA are as follows.

a) Initial reactor operation 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 as follows.

a) RIS accumulator available;

b) MHSI unavailable;

c) LHSI unavailable;

d) Containment spray system unavailable;

e) IVR available;

f) Opening of the SADV when maximum core outlet gas temperature exceeds 650 °C.

13.5.6.2.2.4 SBO

In SBO severe accident, SBO occurs and combines with failure of SBO diesel generators. All of 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 for primary depressurization. Cladding temperature increases quickly and hydrogen is produced by the reaction of zirconium and vapour. Hydrogen is released to the quench tank through the SADV and finally goes to reactor coolant pump compartment in the containment.

Initial conditions for the accident analysis are as follows:

a) Initial reactor operation 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 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) Opening of the SADV when maximum core outlet gas temperature exceeds 650 °C.

13.5.6.2.3 Effectiveness of Mitigation Measures

A preliminary study of the effectiveness of the EUH [CCGCS] is performed through an integral code. Hydrogen is generated in the core and released from the breaks or the SADV into its joint compartments. These compartments often have the peak hydrogen concentration. The present study focuses on the hydrogen risks in these main compartments.

13.5.6.2.3.1 LB-LOCA

a) Without EUH [CCGCS]

For this scenario without EUH [CCGCS], hydrogen generated by zirconium-water reaction cannot be reduced effectively.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], hydrogen generated by zirconium-water reaction can be reduced effectively.

13.5.6.2.3.2 IB-LOCA

a) Without EUH [CCGCS]

For this scenario without EUH [CCGCS], hydrogen generated by zirconium-water reaction cannot be reduced effectively.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], hydrogen generated by zirconium-water reaction can be reduced effectively.

13.5.6.2.3.3 SB-LOCA

a) Without EUH [CCGCS]

For this scenario without EUH [CCGCS], hydrogen generated by zirconium-water reaction cannot be reduced effectively.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], hydrogen generated by zirconium-water reaction can be reduced effectively.

13.5.6.2.3.4 SBO

a) Without EUH [CCGCS]

For this scenario without EUH [CCGCS], hydrogen generated by zirconium-water reaction cannot be reduced effectively.

b) With EUH [CCGCS]

For this scenario with EUH [CCGCS], hydrogen generated by zirconium-water reaction can be reduced effectively.

13.5.6.2.4 Conclusions

The calculation on assessment of EUH [CCGCS] for reference design, HPR1000 (FCG3), has been finished. The conclusion of HPR1000 (FCG3) is that EUH [CCGCS] is effective to reduce hydrogen risk under accident conditions. Calculation for UK HPR1000 is still ongoing. The results and conclusions will be supplemented in supporting documents [33] during Step 3 and PCSR v1 at the entry of Step 4.

13.5.6.3 Assessment of IVR

13.5.6.3.1 Assessment Method

It is required to meet the following criteria to ensure that IVR strategy is effective after severe accidents:

a) The heat flux transferred from the corium to the outer surface of RPV lower head shall be lower than the local CHF;

b) Provided that criterion a) is met, and part of the RPV lower head wall is melted by the core melt, the wall with the minimum thickness still have enough mechanical strength to maintain the RPV integrity.

When the core outlet temperature reaches 650°C, after the primary cooling system 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.

Several steps are taken to assess the effectiveness of IVR, the analysis flow-chart is shown in F-13.5-6.

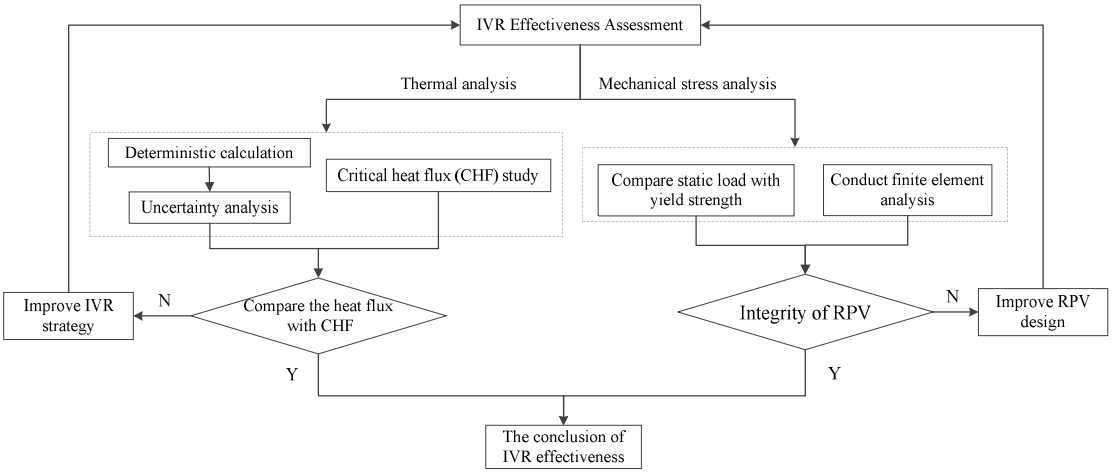
In order to demonstrate the effectiveness of IVR, three issues should be concerned. Firstly, the heat flux from the corium pool to RPV wall is obtained. Secondly, series of IVR related tests are performed to get the critical heat flux (CHF) distribution along the outer surface of RPV. Finally, the mechanical analysis is conducted to evaluate whether the residual wall can sustain the integrity of RPV.

a) Regarding the thermal load calculation, 1) Series of severe accident sequences selected by PSA, deterministic analysis and engineering judgement are analysed. These sequences include LB-LOCA, IB-LOCA, SB-LOCA, ATWS and Station Black Out (SBO) with loss of SBO diesel generators. 2) For the uncertainty analysis, a dedicated code (MOPOL) is used to calculate the heat flux which transfers from corium pool to RPV wall. There are four input parameters for calculating the heat flux, including decay heat in molten pool, fraction of Zr oxide, mass of Fe, fraction of reactor core melt. Probability Distribution Function (PDF) for the key parameters is determined by different severe accident sequences

analysis result.

b) For the critical heat flux, IVR experiments have been conducted to obtain the CHF distribution along the RPV outer surface.

c) For the mechanical stress analysis, there are two major approaches. The first one is comparing static load with yield strength. It is a simple method to evaluate whether the residual wall can keep the integrity of RPV. The second one is finite element analysis. It 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.



F-13.5-6 Flow-chart of the IVR assessment

13.5.6.3.1.1 Method of heat transfer from corium pool to RPV

The two layers 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 the melting point approximately of 2,973K. 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 oxidized zirconium, the fraction of molten core, and the decay heat of the corium pool.

13.5.6.3.1.2 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.

13.5.6.3.1.3 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 corium pool forms, the mechanical stress calculation has been conducted.

If the initiating sequence of 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 inner and outer of primary loop can be neglected when 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 primary loop also decreases rapidly after the SADV is opened. So the inner pressure 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 concludes 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 RPV should also be considered. The yield strength can be obtained according to 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. So we can evaluate the safety margin of mechanical stress 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 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 if 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 Input Parameters for Calculation

As is known from Sub-chapter 13.5.6.3.1, the input parameters for IVR effectiveness evaluation are as follows: 1) RPV geometry parameters; 2) CHF curve of the RPV outer surface; 3) the mass of molten stainless steel, the fraction of oxidized zirconium, the fraction of molten core, and the decay heat of the corium pool.

13.5.6.3.2.2 Calculation and Analysis on Heat Transfer in RPV Lower Surface

During severe accidents, the corium will finally collapse into the RPV lower head. To determine heat flux distribution of the RPV outer surface, the three key parameters are as follows:

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-oxidized 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.

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. It must be noted that:

a) The thickness of the metal layer is a key parameter which determines whether IVR strategy is effective. Due to heat focusing effect, the thinner the metal layer is, the higher the probability of RPV failure will be.

b) As for the impact of the oxide layer on heat transfer, the higher the oxide layer volume, the lower the heat flux on the wall.

c) The decay heat in the oxide pool acts as heat source of corium pool.

If the cooling water is capable of removing the heat from the out surface of RPV to prevent the process of corium erosion, the IVR strategy is successful.

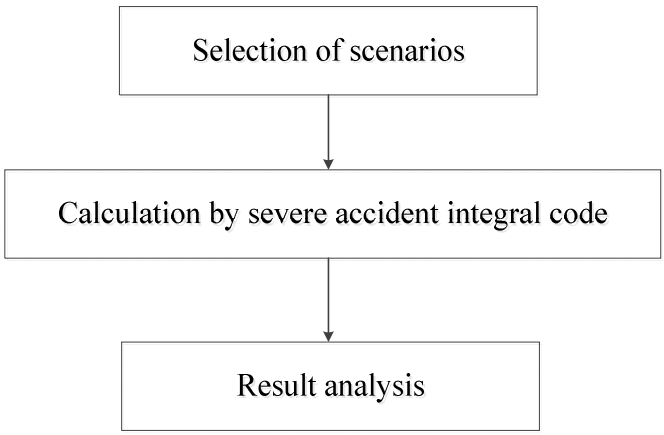
13.5.6.3.3 Conclusion

The calculation on assessment of IVR for reference design, HPR1000 (FCG3), has been finished. The conclusion of HPR1000 (FCG3) shows that reactor pit flooding system can retain the corium inside the RPV with a very high level of confidence. Calculation for UK HPR1000 is still ongoing. The results and conclusions will be supplemented in supporting documents [34] during Step 3 and PCSR v1 at the entry of Step 4.

13.5.6.4 Assessment of the EHR [CHRS]

13.5.6.4.1 Method for the Assessment of the EHR [CHRS]

Several steps are taken to assess the EHR [CHRS], the analysis flow-chart is as follows:



F-13.5-7 The flow-chart of the EHR [CHRS] assessment

1) Selection of relevant scenarios

For assessment of the EHR [CHRS], according to the accident sequence selection results in Sub-chapter 13.5.5.2.3.3 and Table T-13.5-4, the LB-LOCA is chosen, which is the accident sequence with the fastest accident progression and fastest early-stage containment pressure increase which is an enveloping accident sequence for the containment overpressure response analysis.

2) Calculation by severe accident analysis code

Calculations are performed by ASTEC, and the description of the code has been given in Appendix 13A.

3) Result analysis

During the assessment of the EHR [CHRS], 12 h after the severe accident, the EHR [CHRS] is started and the pressure in the containment begins to drop due to the spray effect. The criteria of the effectiveness assessment is that the EHR [CHRS] can maintain the pressure in the containment below the containment design pressure of 0.52 MPa (one train), reduce the pressure below { } in less than 24 h and keep the pressure at a value lower than { } (two trains). The effectiveness of the EHR [CHRS] can be justified by comparing the calculation results to the criteria of effectiveness assessment.

13.5.6.4.2 Event Description

The LB-LOCA scenario at power condition is the accident sequence with the fastest accident progression and fastest early-stage pressure increase in the containment. As the start-up threshold of the IVR strategy is reached earlier for this event, the decay heat is higher, the vapour generated after the IVR is larger and containment pressure increase is faster. More mass and energies released to the containment more challenges to the containment, thus the LB-LOCA is selected as the enveloping accident sequence for the containment overpressure response analysis.

The initial conditions for the accident analysis are as follows.

1) Initial reactor operation 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, and only the RIS accumulator is available;

2) MCD unavailable;

3) LCD unavailable;

4) ASG [EFWS] unavailable;

5) When the core outlet temperature reaches 650°C, the IVR is manually started;

6) Two trains/one train of the EHR [CHRS] are manually started to remove the heat in the containment 12 h after the core outlet temperature reaches 650°C;

7) The inlet water temperature of the cold side (heat sink) in the EHR is 45°C, and its flowrate is 360 m^3/h. The flowrate of the hot side is 330 m^3/h.

13.5.6.4.3 Effectiveness of mitigation measures

Calculations are performed by ASTEC, and the description of the code has been given in Appendix 13A.

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, thus leading to containment failure in the long term.

b) LB-LOCA with 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) 12 h after the core outlet temperature reaches 650°C, two trains / one train of the EHR [CHRS] are/is manually started to remove heat from the containment and the pressure in the containment begins to drop due to the spray effects. If two EHR [CHRS] trains are started the containment pressure can be reduced to below { } within 24 h after system activation. If one EHR [CHRS] train is started, the containment pressure is kept below the design pressure.

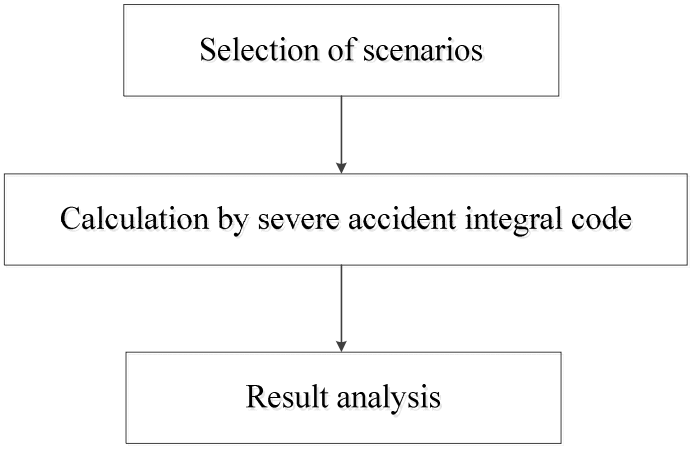
13.5.6.4.4 Conclusions

The calculation on assessment of EHR [CHRS] for reference design, HPR1000 (FCG3), has been finished. The conclusions of HPR1000 (FCG3) are that the containment pressure remains clearly below the containment design pressure under LB-LOCA accident, and the design of 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. Calculation for UK HPR1000 is still ongoing. The results and conclusions will be supplemented in supporting documents [35] during Step 3 and PCSR v1 at the entry of Step 4.

13.5.6.5 Assessment of EUF [CFES]

13.5.6.5.1 Method for the Assessment of EUF [CFES]

Several steps are taken to assess the EUF [CFES], the analysis flow-chart is as follows:



F-13.5-8 The effectiveness assessment procedure of EUF [CFES]

a) Selection of relevant scenarios

Extremely unlikely conditions are considered, such as long term loss of all AC power with LB-LOCA (Conservative, to make containment pressure increase early, assuming LB-LOCA as the initial accident according to the selected sequence in Table 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 valid 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 has been given in Appendix 13A.

c) Result analysis

The analysis results are shown in 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, the detailed descriptions are as follows.

The initial conditions for the accident analysis are as follows.

a) Initial reactor operation 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

Calculations are performed by ASTEC, the accident progression for the LB-LOCA case with the EUF [CFES] and without the EUF [CFES] are described as follows.

a) LB-LOCA with EUF [CFES]

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. When the pressure exceeds 0.52 MPa abs., 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 deceases 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.

b) LB-LOCA without EUF [CFES]

If the containment pressure exceeds 0.52 MPa abs., with the failure of EUF [CFES], the containment will fail due to overpressure.

13.5.6.5.4 Conclusions

The calculation on assessment of EUF [CFES] for reference design, HPR1000 (FCG3), has been finished. The conclusion of HPR1000 (FCG3) is that EUF [CFES] is effective to control containment pressure under accident conditions. Calculation for UK HPR1000 is still ongoing. The results and conclusions will be supplemented in supporting documents [36] during Step 3 and PCSR v1 at the entry of Step 4.

13.5.7 Severe Accident in Spent Fuel Pool

Fuel melt scenarios in spent fuel pool and the potential fission product release will be analysed and presented in PCSR v1.

13.5.8 Source Term Evaluation of DEC-B events

Level 2 PSA source terms are analysed for the evaluation of DEC-B events, which includes all results of representative sequences in severe accidents.

The Level 2 PSA source terms analysis includes release time, magnitude, physical and chemical characteristic, height and frequency of all Release Categories (RCs). Release categories are based on the release time and the magnitude of fission products. Level 2 PSA source terms are applied to release targets analysis and Level 3 PSA.

13.5.8.1 Analysis Method

The consideration of containment release paths is coordinated with the Level 2 PSA. Since the Containment Event Trees (CETs) have a large number of end states, for

simplification reasons, the end states are required to be grouped into RCs which provide an effective interface between the Level 2 PSA and Level 3 PSA. The source terms analysis will be carried out for the RCs by representative severe accident sequences. The process of the source terms analysis is the following:

a) Specifying the RCs;

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

c) Identifying the representative of each RC;

d) Carrying out source terms analysis for the RCs using ASTEC.

The contents related to accident chemistry and severe accident source terms are described in the accident chemistry methodology reports [42].

13.5.8.2 Results

The Sub-chapter will be supplemented in PCSR v1.

13.5.9 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 insignificant level.

13.5.9.1 Methodology of Practical Elimination Demonstration

An early or large radioactive release caused by accident sequences or phenomena 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 targets defined in the General Safety Requirements [22] should be satisfied.

The process of practical elimination demonstration is shown in Figure F-13.5-9 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 releases. The source of an early or large radioactive release includes the reactor core and the spent fuel pool. For the 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 the 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, and

d) Release path from base melt through.

In UK HPR1000, the following accident sequences or phenomena may lead to the early or large radioactive releases.

a) MCCI

b) DCH

c) Hydrogen combustion and explosion

d) Steam explosion

e) Containment overpressure

f) Large reactivity insertion

g) Containment isolation failure

h) Containment bypass

i) 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.

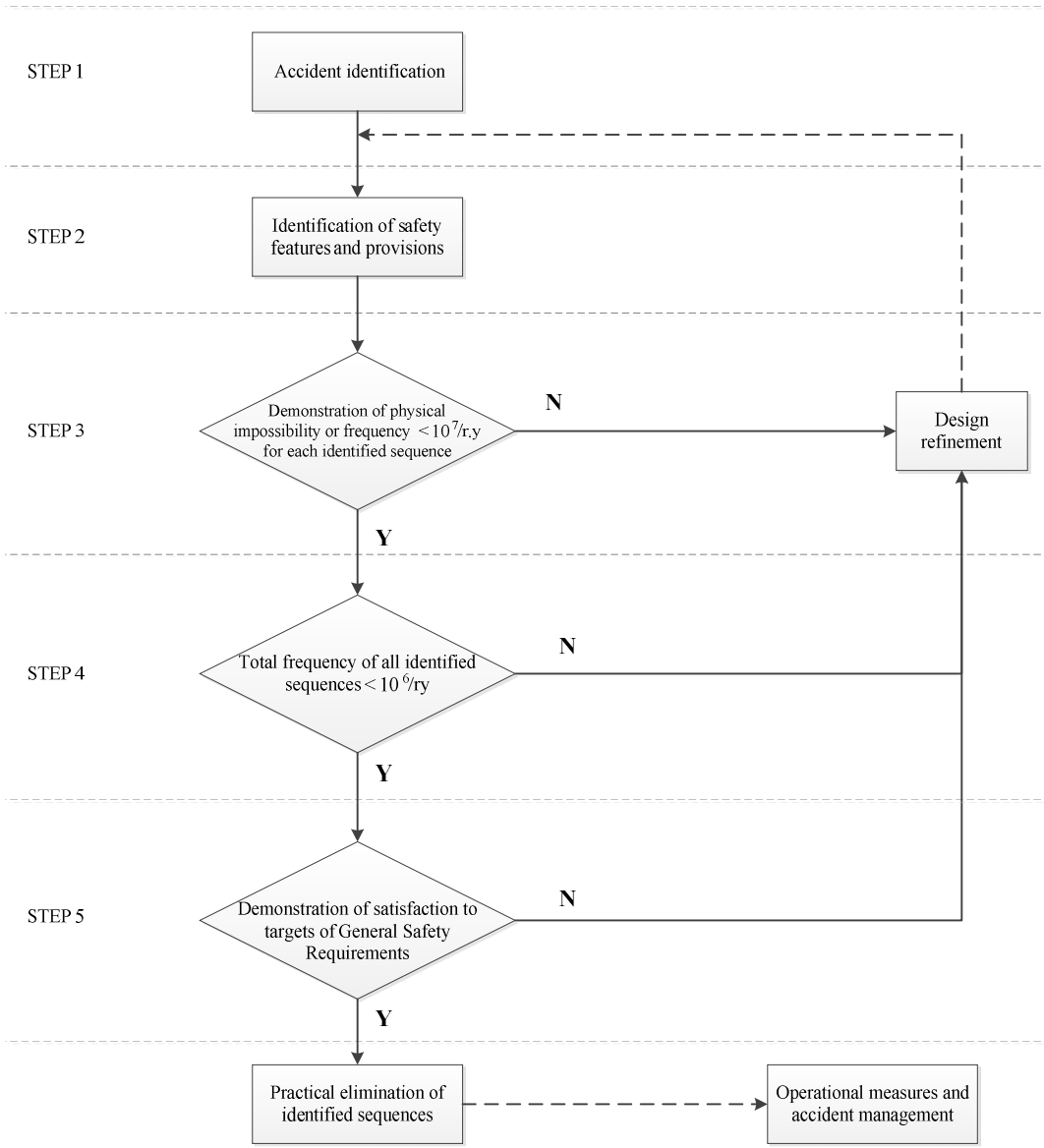
Step 3 is the demonstration of practical elimination of the early or large radioactive releases caused by each identified accident sequence or phenomenon via ‘physically impossible’ or ‘extremely unlikely’. If the early or large radioactive release cannot be demonstrated to be practically eliminated, design refinements will be considered.

Step 4 is the demonstration that the total frequency of identified accident sequences or phenomena is lower than 10^{-6} 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 to targets defined in the General Safety Requirements [22]. In this step Level 3 PSA results will be used.

Practical elimination is demonstrated after these five main steps. 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 accident management measures are supposed to be implemented.



F-13.5-9 Flow-chart of Practical Elimination

13.5.9.2 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 total frequency and radiological consequence of all identified accident sequences and phenomena will be added together. If the total frequency is lower than 10^{-6} per reactor year and the radiological consequence assessment satisfies the targets defined in the General Safety Requirements [22], it can be concluded that an early or large radioactive release caused by the accident sequences or phenomena can be considered practically eliminated [37].

13.5.10 Severe Accident Environmental Conditions

The EHR [CHRS] and EUF [CFES] have significant influence on the containment temperature and pressure under severe accident. According to the functions of these two systems, the severe accident environmental conditions in the containment of the UK HPR1000 include two situations:

a) The EHR [CHRS] is available;

b) Active functions of the EHR [CHRS] are lost and the EUF [CFES] is available.

13.5.10.1 Accident sequences analysis

The accident sequences for calculating the severe accident environmental conditions are selected from the typical severe accident sequences and include the following situations based on whether the active functions of the EHR [CHRS] are available:

a) The EHR [CHRS] is available;

The accident sequences of LB-LOCA, SB-LOCA, SBO and ATWS are calculated and analysed to cover different processes.

b) Active functions of the EHR [CHRS] are lost and the EUF [CFES] is available.

Active functions failure of the EHR [CHRS] means that the passive IVR is effective while the active IVR and containment spray functions are lost. The other assumptions for the accident analysis are shown in Sub-chapter 13.5.6.5. In the Sub-chapter, long term loss of all AC power with LB-LOCA is selected as a conservative accident sequence in the case of the EUF [CFES] being available.

13.5.10.2 Results

The environmental condition curves derived from ASTEC results will be presented in PCSR v1.

13.5.11 Basic Strategy of Severe Accident Management Guideline (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 ensure 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.

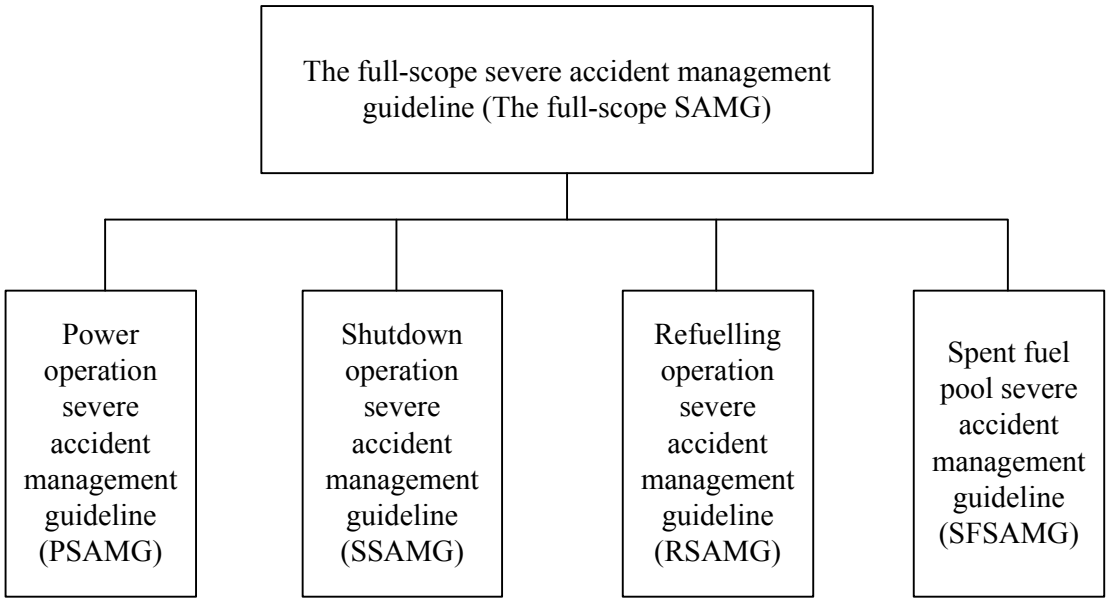
The transition from the EOP to SAMG is based on the core outlet temperature and/or dose rate in the containment (water level and/or dose rate in the SFP). These criteria are continuously monitored whilst the EOP is in progress. When the entry criterion is reached, the SAMG is used instead of the EOP. The decision of using the SAMG is made by a duly authorised person according to the requirements in the UK.

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 [38], 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 [39].

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.

13.5.11.1 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-13.5-10 [40].



F-13.5-10 Framework of the full-scope SAMG

13.5.11.2 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 ensuring 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 decide which mitigation strategies should be implemented according to the parameters. Besides, typical calculation aids will be given in advance, which can greatly improve the analysis and judgment abilities of the TSC technicians.

Moreover, 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, way of heat removal, containment state, effectiveness of mitigation strategies and offsite release controlling strategies, and whether failed systems have been restored or not [41].

13.5.12 Lessons Learnt from Fukushima Accident

After the Fukushima accident, CGN undertook a review based on the analyses of the accidents, the international lessons learnt from the accident, the relevant guidance documents and good practices, and also the lessons learned from the review of operating reactors in China.

Some important relevant documents are listed below:

a) European Nuclear Safety Regulators Group (ENSREG), "EU 'Stress Tests' Specifications, Annex 1", May 2011.

b) Office for Nuclear Regulation (ONR), "Japanese Earthquake and Tsunami: Implications for the UK Nuclear Industry, Interim-report", May 2011.

c) ONR, "Japanese Earthquake and Tsunami: Implications for the UK Nuclear Industry, Final Report", September 2011.

d) IAEA, "International Fact Finding Expert Mission of the Fukushima Daiichi NPP Accident Following the Great East Japan Earthquake and Tsunami", June 2011.

e) IAEA, "Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant", March 2012.

f) IAEA, "Severe Accident Management in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant", March 2014.

g) Nuclear Energy Agency/Committee on Nuclear Regulatory Activities (NEA/CNRA), "Accident Management Insights after the Fukushima Daiichi NPP Accident", February 2014.

From the insights of the documents mentioned above, a number of important recommendations should be assessed:

a) Design basis and margins for flooding and earthquake, etc.;

b) Operational capability of structures, systems and components required for the management and control of an accident;

c) Diverse means of providing robust sufficiently long-term independent electrical supplies and cooling means;

d) On-site emergency control, instrumentation, and communications in light of the

circumstances of the Fukushima accident;

e) Severe accident management measures, such as core cooling, spent fuel cooling, containment integrity, necessary water make-up strategies, etc.

On the other hand, some significant plant-specific improvements are identified according to the EU 'Stress Tests', such as seismic upgrades and flood protection physical features to improve robustness. The most promising improvements being considered by many countries are additional power and water supplies to be provided by mobile equipment, for which the connecting arrangements would be established in advance, additional sources of water, extended or additional supplies of fuel, valve line-up accessibility as well as various operational improvements.

In China, the National Nuclear Safety Administration (NNSA) had also implemented a series of inspections after the Fukushima accident, and finally published a report which paid close attention to eight fields. Hence, the HPR1000 (FCG3) design has already thought over extreme events like the Fukushima accident which lead to a complete and extended loss of power and infrastructure damage. These include:

a) Design against flooding events

The design basis flooding level has considered the beyond design basis external flooding, and the potential flooding level introduced by a tsunami has been covered.

b) Emergency water makeup

Generally, three important water makeup means should be taken into account:

1) Injection to the primary loop to restore core cooling. This strategy is designed through the EHR [CHRS]-RIS [SIS] piping using mobile pumps;

2) Makeup to the SFP via water pool of the Secondary Passive Heat Removal System (ASP [SPHRS]);

3) Emergency water makeup to related SGs by the ASP [SPHRS] to remove decay heat in the SGs.

It should be noted that, all three strategies are designed to have connection points for portable makeup pumps.

c) Flexible electrical supply

Sufficient defence in depth is applied in the design of the electrical power systems. The plant is equipped with three EDGs, two SBO diesel generators and a mobile diesel generator which significantly improves the flexibility of the electrical supply. In the case of a total loss of AC power, the ASP [SPHRS] is designed to remove the residual heat of the reactor core from the secondary side passively.

d) Monitoring system in the SFP

Significant parameters in the SFP such as water level and temperature are monitored continuously, with a robust electrical supply and measurement range.

e) Hydrogen monitoring and control system

Based on various calculations, the specific system of the EUH [CCGCS] is designed to help reduce the hydrogen risk and maintain containment integrity under severe accident conditions.

f) Habitability of emergency control centre

The emergency control centre is located in a seismic class 1 structure which can also withstand the Design Basis Flood (DBF). Furthermore, the HPR1000 (FCG3) optimises ventilation systems to make sure that the radiation dose is less than 100mSv during the whole emergency period (usually about 30 days).

g) Radiation monitoring and emergency response

Monitoring equipment and spots should be reasonable and representable. The HPR1000 (FCG3) has installed a γ monitoring station, environment laboratory, environment monitoring wheeled machine and a thermoluminescent dosimeter. On the other hand, regular exercises and drills should be taken into account.

h) External hazard

Improved measures, such as a watertight seal and breakwater, are designed to cope with the effects of the DBF level and a thousand-year return period rainfall.

The nuclear power plant operation organisation strengthens the bonds and information exchange with the meteorological, marine and seismological bureaus.

In the development process of the HPR1000 (FCG3), the lessons learnt from the Fukushima accident have been taken into account, and a number of design modifications and improvements have been proposed. The UK HPR1000 takes the HPR1000 (FCG3) as the reference design, and these improvements are also addressed in the design of the UK HPR1000. A comprehensively assessment will be given in GDA Step 3 and Step 4.

13.6 ALARP Assessment

13.6.1 Scope of ALARP

According to the 2014 Safety Assessment Principles (SAPs), the SAA should consider questions like ‘what more can reasonably be done?’ or ‘what would need to be done in such an event?’. The ALARP evaluation needs to be performed to ensure that the risk to the UK HPR1000 from severe accidents is ALARP. The relevant good practice is 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 rationale for the choice of each of the mitigation measures will be described in the 'Severe Accident Engineered Measures Summary Report' which will be produced at the beginning of Step 4 of GDA.

The purpose of the SAA ALARP assessment will be 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 practical.

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 Approach and Main Process of ALARP Assessment

During the ALARP assessment that will be carried out during the GDA, the potential risk assessment, relevant good practice identification and optioneering process are the main elements.

The first step is identification of relevant good practice. In the descriptions of the mitigation systems above, it is discussed whether the design parameters and overall system design is already consistent with RGP in some cases.

The approach adopted in further ALARP assessments of the individual systems will depend on the system. For some systems it may just be a case of optimisation. But for other systems a balance may need to be achieved as reducing risk in one area may increase risk in another. In the latter case, an optioneering process will be used where performance against different attributes will be scored with appropriate weightings. The ALARP Methodology Report, which has been submitted to the ONR, provides more details on the optioneering process that will be applied for the UK HPR1000.

Attributes that may be considered in the SAA ALARP optioneering could include: off-site risk in short and long term, worker risk, societal risk, economic consequences of an accident, environmental impact etc.

For the EUH [CCGCS], the performance of the system with regards to hydrogen control is determined by the number, capacity, and location of the combiners. The ALARP assessment for this system will involve a performance assessment using the methodology described in Sub-chapter 13.5.6.2 above with an increased number and modified positions of combiners and the resulting performance compared with that of the current configuration. There may be scope for further improvements in terms of choice of design and manufacture of the individual combiners but these could be considered by the future licensee during site licensing.

For the EUF [CFES], an optioneering process may be required as risks need to be balanced. Venting the containment reduces the risk of containment failure and a large release of radioactivity to the environment but involves a certain small release of radioactivity to the environment. The optioneering here will consider the optimum pressure at which to vent – too high and the containment might fail and too low and activity may be released unnecessarily. There may also be scope for improvements in the design and type of filters to be employed; this could be further considered during site licensing.

For the SADV, the valve capacity and time delay are the key factors. The performance of the valve can be evaluated and optimised according to the depressurising rate, grace period and primary pressure when the RPV fails.

For the IVR, the effects of possible improvements will be investigated using the test rig facility or the computer analysis described in Sub-chapter 13.5.6.3 above. Improvements that might be considered including an increase in the IVR tank capacity, increase in the flow rate, etc.

For the EHR [CHRS], variations in system parameters will be assessed. Analysis on the capacity and redundancy of pumps and heat exchanger may be required. The limiting parameters could be the decay heat after accidents, the ambient condition, etc.

For the SFP, as the consequence of fuel melt is unacceptable, the risk of fuel uncover needs to be assessed to determine if there are further reasonable improvements on the PTR [FPCTS]. The maximum possible decay heat in the SFP, the potential drainage flowrate, the period for power and cooling recovery, and the temperature limitation of pump need to be considered.

For the design as it is, a risk assessment will be performed. The potential risks related to severe accidents will be identified based on insights from the PSA, experience from the reference design and expert judgement. Risk-dominant sequences will be closely examined to determine if there is scope for further risk reduction; this will be followed by the next largest contributors. The examination will involve revisiting the

optimisation or optioneering carried out for the individual systems considering whether any performance criteria or any weighting/scoring needs to be a reassessed. The assessment will be informed by a consideration of the consequences and frequencies of the scenario to form a judgement over whether: the risks are real and a good best-estimate, subject to large uncertainty, or are a result of possibly excessive conservatisms.

If any improvements are identified, the practicality of implementing the measure will be evaluated and compared with the risk reduction achievable to determine whether this would be an ALARP solution or not. If so, it will be incorporated in the design.

13.7 Concluding Remarks

Chapter 13 presents the following aspects of design extension conditions of the UK HRP1000:

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 effect beyond design basis is proven to be eliminated.

With probabilistic and deterministic methods combined engineering judgement, 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.

13.8 References

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

[2] CGN, Methodology of DEC-A Identification, GHX00100068DOZJ03GN, Rev. A, 2018.

[3] CGN, The Design Condition List and Acceptance Criteria, GHX00100029DOZJ04GN, Rev. D, 2018.

[4] CGN, Methodology of DEC-A Analysis, GHX00600175DRAF02GN, Rev. B, 2018.

[5] CGN, Total Loss of Feedwater Accident Analysis, GHX00600074DRAF02GN, Rev. B, 2018.

[6] CGN, Small Break Loss of Coolant Accident with Loss of Medium Pressure Rapid Cooldown, GHX00600096DRAF02GN, Rev. B, 2018.

[7] CGN, Small Break Loss of Coolant Accident with Total Loss of Low Head Safety Injection, GHX00600098DRAF02GN, Rev. B, 2018.

[8] CGN, Station Blackout Accident Analysis (State A), GHX00600025DRAF02GN, Rev. B, 2018.

[9] CGN, Station Black Out in Shutdown Condition, GHX00600026DRAF02GN, Rev. B, 2018.

[10] CGN, PTR aspects in the Station Blackout condition (all states), GHX00600117DRAF02GN, Rev. B, 2018.

[11] CGN, ATWS by Rods Failure-Loss of Main Feedwater, GHX00600078DRAF02GN, Rev. B, 2018.

[12] CGN, ATWS by Rods Failure-Loss of offsite Power, GHX00600031DRAF02GN, Rev. B, 2018.

[13] CGN, Small Break Loss of Coolant Accident with Total Loss of Medium Head Safety Injection, GHX00600097DRAF02GN, Rev. B, 2018.

[14] CGN, Total Loss of Cooling Chain (State A), GHX00600119DRAF02GN, Rev. B, 2018.

[15] CGN, Total Loss of Cooling Chain in Shutdown Condition, GHX00600120DRAF02GN, Rev. B, 2018.

[16] CGN, Uncontrolled primary water level drop without SI signal from Reactor Protection System (RPS) (state D), GHX00600206DRAF02GN, Rev. A, 2018.

[17] CGN, Multiple Steam Generator (SG) tubes rupture (10 tubes) (State A), GHX00600086DRAF02GN, Rev. B, 2018.

[18] CGN, Main Steam Line Break (MSLB) with Steam Generator Tube Rupture (SGTR) (1 tube) in the affected SG (State A), GHX00600080DRAF02GN, Rev. B, 2018.

[19] CGN, SGTR (1 tube) with Atmospheric Steam Dump System (VDA [ASDS]) stuck open in the SG affected (State A), GHX00600087DRAF02GN, Rev. B, 2018.

[20] NRC, Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors, RG 1.183, July 2000.

[21] NRC, Iodine Behavior in a PWR Cooling System Following a Postulated Steam Generator Tube Rupture Accident, NUREG-0409, May 1985.

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

[23] CGN, Safety case strategy of severe accident analysis, GHX00600177DRAF02GN, Rev. B, 2018.

[24] CGN, Overall methodology of severe accident analysis, GHX00600007DRAF02GN, Rev. B, 2018.

[25] Nuclear Regulatory Commission. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, NUREG-75/0114 (WASH-1400), 1975.

[26] Nuclear Regulatory Commission. A Review of the Current Understanding of the Potential for Containment Failure from In-Vessel Steam Explosions, NUREG-1116 (SERG-1 Report), 1985.

[27] OECD/NEA and UCSB. Proceedings of the CSNI Specialists Meeting on Fuel-Coolant Interactions, NUREG/CP-0127 (NEA/CSNI/R(93)8), 1993.

[28] 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.

[29] OECD/NEA/CSNI. OECD Research Program On Fuel-Coolant Interaction Steam Explosion Resolution For Nuclear Applications – SERENA-1 Final Report, NEA/CSNI/R (2007)11, 2007.

[30] EUR, European Utility Requirements for LWR Nuclear Power Plants - Volume 2 Generic Nuclear Island Requirements: Chapter 1 Safety Requirements, Revision D, October 2012.

[31] CGN, Selection of Severe Accident Scenarios, GHX00600058DRAF02GN, Rev. C, 2018.

[32] CGN, Depressurization Capacity Analysis of Severe Accident Dedicated Valve, GHX00600055DRAF02GN, Rev. B, 2018.

[33] CGN, Assessment of containment combustible gas control system by lumped parameter method, GHX00600103DRAF02GN, Rev. B, 2018.

[34] CGN, Assessment of In-Vessel Retention Strategy, GHX00600113DRAF02GN, Rev. B, 2018.

[35] CGN, Assessment of EHR [CHRS], GHX00600063DRAF02GN, Rev. B, 2018.

[36] CGN, Assessment of EUF [CFES], GHX00600065DRAF02GN, Rev. B, 2018.

[37] CGN, Practically eliminated situations, GHX00600127DRAF02GN, Rev. C, 2018.

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

[39] IAEA, Severe Accident Management Programmes for Nuclear Power Plants, NS-G-2.15, 2009.

[40] CGN, General Study Report for Full-scope SAMG, GHX00600121DRAF02GN, Rev. B, 2018.

[41] CGN, Technical Scheme and Framework Development Report for Full-scope SAMG, GHX00600122DRAF02GN, Rev. B, 2018.

[42] CGN, Methodology of Accident Chemistry, GHX00100002DRAF03GN, Rev. B, 2018.

Appendix 13A Computer Codes Used in the DEC-A and DEC-B Analysis

In the DEC-A analysis, LOCUST, GINKGO and LINDEN are used. The information of these codes 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. Dedicated codes used are GASFLOW, COM3D, MC3D and MOPOL.

ASTEC

The ASTEC code (Accident Source Term Evaluation Code) aims at simulating the behavior 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 has been initiated end of 2009 in the particular frame of SARNET network and it has been then intensively continued.

GASFLOW

GASFLOW is a computational fluid dynamics code which is a best-estimate tool to characterize local phenomena within a flow field. GASFLOW can be used to predict the transport, mixing, and combustion of hydrogen and other gases, liquid water droplets, and aerosols in nuclear reactor containments and other nonnuclear buildings.

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.

COM3D

COM3D is a three-dimensional code for turbulent reactive flow simulations in complex 3D-geometries. The Favre averaged Navier-Stokes equations are solved together with different models for turbulence and chemical kinetics.

COM3D is developed by Karlsruhe Institute of Technology and it has been used to perform hydrogen safety analysis of Fangchenggang units 3&4, etc.

COM3D can be used to assess the dynamic pressure loads in the containment during fast combustion.

The code was validated and verified by several tests include: (1) Forward facing step problem, (2) He-air turbulence test in the FZK shock tube, (3) Reactive flow tests in different scales in the FZK shock tube, (4) Large scale experiments performed in the RUT facility. The computational results are in agreement with the test results.

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 however able to calculate very different situations and has a rather wide field of potential applications.

The MC3D code is developed by IRSN. It has been used to analysis the risk of steam explosion 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 PRELEMANGE, 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 was calculated based on the heat transfer model in the molten pool.

MOPOL is developed by CGN and Shanghai Jiaotong 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.